Gigaset
SE366 WLAN

XSPAN™ ATHEROS

Indice

Avvertenze di sicurezza 6

Il vostro contributo alla protezione ambientale (ECO) 6

Il Gigaset SE366 WLAN 7

Reti locali con prodotti Gigaset 8
- Rete locale via cavo (Ethernet) 9
- Rete locale wireless (WLAN) 10
- Collegamento della rete wireless (WLAN) con Ethernet (LAN) 12
- Funzioni di sicurezza 13
- WPS 13

Prestazioni e possibilità d'impiego 15
Procedimento per l'installazione e la configurazione 17

Procedure iniziali 18

Contenuto della confezione 18
Requisiti del sistema 18
Spie luminose e collegamenti 19
- lato anteriore 19
- Lato posteriore 20

Posizionamento del Gigaset SE366 WLAN 21
- Avvertenze per l'uso 22

Collegare il Gigaset SE366 WLAN 22
- Collegare al modem DSL o via cavo 22
- Collegare alla rete elettrica 23
- Collegare i PC wireless tramite WPS 23
- Collegamento cablato ad un PC 24
- Collegare wireless ad un PC senza WPS 25

L'interfaccia operativa 26

Avvio dell'interfaccia operativa 26
La pagina iniziale 27
Scelta della lingua 29
Elementi dell'interfaccia operativa 29

Impostazioni di base 31

Opzioni regionali 31
Configurazione della connessione a Internet 32
Riepilogo 34

Impostazioni di sicurezza 35

Cambiare la Password 35
SSID 37
Impostazione delle funzioni di protezione per rete wireless 38
WPA2 / WPA con Pre-shared Key (PSK) 39
Crittografia WEP 40
Controllo di accesso nella rete wireless 42
Salvataggio delle impostazioni 43

Configurazione delle Impostazioni avanzate 44

Configurazione della connessione Internet 45
Internet 45
Connessione Internet 45
Server DNS 49
Indirizzo MAC 49
Firewall 50
Protezione dagli hacker 51
Impostazione del controllo di accesso a Internet 53
Impostazione della funzione NAT 56
Port-Triggering 58
Inoltro porte 59
Apertura del firewall per determinati PC (Host esposto) 60
DNS dinamico 61
QoS (Quality of Service) 62
Configurazione LAN 63
Assegnazione di indirizzi IP statici a singoli PC 65
Configurazione per connessioni wireless 65
Impostare WPS 68
Impostare la crittografia 69
WPA2-PSK e WPA2-PSK / WPA-PSK 69
Crittografia WEP 71
Client ammessi 74
Funzione Ripetitore (WDS) 75

Amministrazione e informazioni sullo stato 77

Istituzione manuale di connessioni Internet 77
Opzioni regionali 78
Orario Internet 79
Password del sistema 79
Impostazione della Gestione remota 80
Salvataggio e ripristino della configurazione 82
Salvataggio dei dati di configurazione 82
Ripristino del backup 82
Ripristino delle impostazioni iniziali 83
Reboot 83

Aggiornamento firmware 84
System Log 85
Disattivare il tasto di registrazione WPS 86

Informazioni sullo stato 87

Panoramica 87
Sicurezza 88
Internet 89
Rete locale 90
Rete wireless 91
Dispositivo 92

Appendice 93

Disattivazione del proxy HTTP e configurazione del blocco dei popup 93
Ricerca errori 95
Specifiche 101
CONFORMITÀ CE 102
Smaltimento 103
Servizio Clienti (Customer Care) (Italia) 104
Servizio Clienti (Customer Care) (Svizzera) 105
Open Source Software 106

Glossario 107

Indice dei lemmi 120

Avvertenze di sicurezza

- Utilizzare esclusivamente l'alimentatore fornito con l'apparecchio.
- L'apparecchi è previsto solo per l'uso in ambienti chiusi (campo di temperatura: da 0 a 40 °C). Evitare l'uso in ambienti umidi o bagnati, polverosi o in presenza di vapori.
- Collegare l'apparecchio con un cablaggio LAN che si trovi solo in ambienti chiusi.
- L'apparecchio può creare interferenze con le apparecchiature medicali.
- Se si cede l'apparecchio a terzi, consegnare anche le istruzioni d'uso e il CD.

Il vostro contributo alla protezione ambientale (ECO)

Noi della Gigaset Communications GmbH costruiamo i propri prodotti con il massimo rispetto possibile per l'ambiente. Il nostro obiettivo è un processo permanente che ci faciliti il rispetto delle rigide norme ISO 14001 per la gestione internazionale dell'ambiente.

Ulteriori vantaggi per l'ambiente

- Grazie ad un alimentatore switching, i nostri router e repeater consumano fino al 60 % in meno di corrente offrendo così una maggiore efficienza energetica.
- In tutti i router e repeater e in alcuni client WLAN, a seconda del singolo apparecchio e del sistema operativo del PC, è possibile ridurre la potenza di trasmissione WLAN.
- La WLAN può essere anche disattivata del tutto.

Marchi di fabbrica

Gigaset Communications GmbH is a trademark licensee of Siemens AG.

Microsoft, Windows Vista, Windows XP, Windows 2000 e Internet Explorer sono marchi registrati di Microsoft Corporation.

Mozilla Firefox è un marchio registrato di Mozilla Organization.

Il Gigaset SE366 WLAN

Il Gigaset SE366 WLAN è un apparecchio potente ma di facile utilizzo per la connessione wireless del PC (WLAN) oppure della propria rete locale (LAN) con Internet (tramite modem DSL o via cavo).

È possibile collegare il PC wireless al Gigaset SE366 WLAN e creare una rete locale wireless (WLAN). Affinché la rete sia sicura, il traffico viene crittografato sulla base dello standard WPA oppure WEP a 64-/128-Bit.

Il Gigaset SE366 WLAN consente l'accesso a Internet a più utenti contemporaneamente. Pertanto, se il proprio Operatore di rete lo consente, è possibile utilizzare un unico account utente. Se si desidera navigare in Internet a costi ridotti, il Gigaset SE366 WLAN rappresenta una soluzione comoda e semplice.

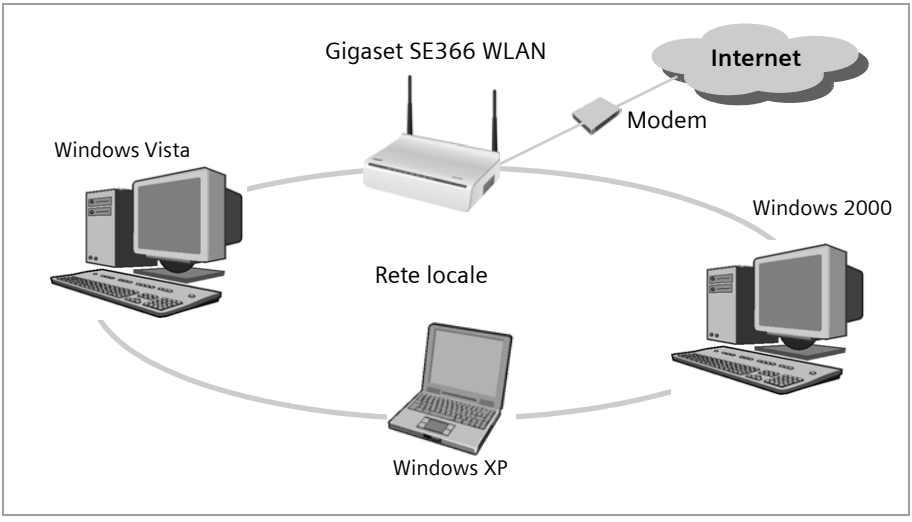
All'interfaccia WAN del Gigaset SE366 WLAN è possibile collegare un modem DSL oppure via cavo.

Nonostante le numerose funzioni, il Gigaset SE366 WLAN è facile da utilizzare anche per i non esperti. Bastano pochi minuti per configurarlo e metterlo in funzione.

Per il collegamento wireless di PC o notebook è disponibile la nuova funzionalità WPS che si può attivare con il tasto di registrazione. Se gli altri client della rete wireless dispongono di WPS, come ad esempio il Gigaset PC Card 300, è allora possibile stabilire la connessione tramite un solo clic (1 click only).

Reti locali con prodotti Gigaset

Grazie al Gigaset SE366 WLAN è possibile creare una rete locale, per es. una rete domestica. Tutti i PC della rete possono comunicare tra loro e hanno accesso a Internet.



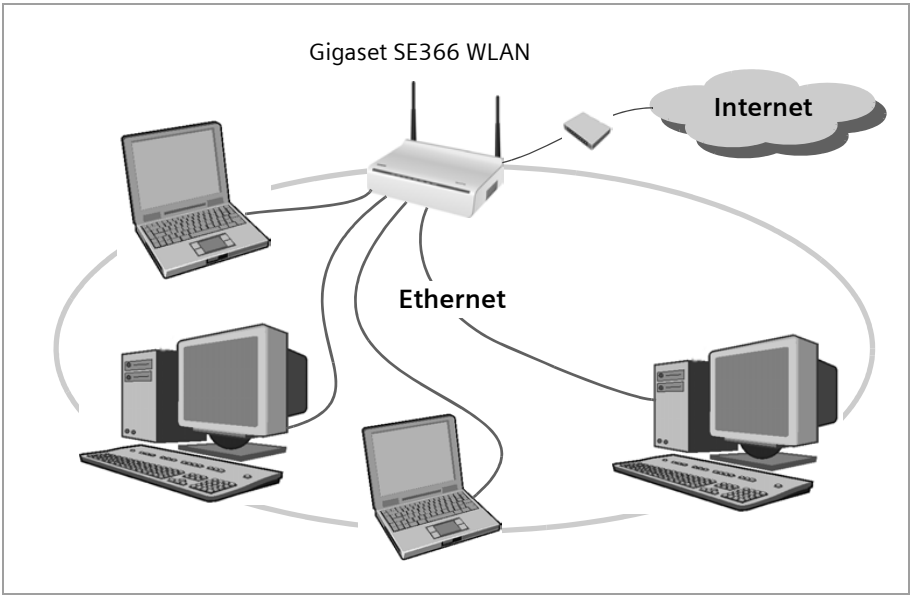
Ci sono diverse possibilità di creare la rete con un Gigaset SE366 WLAN. È possibile

- impostare una rete locale via cavo (Ethernet) e consentire l'accesso a Internet ai PC collegati (v. pag. 9).
- impostare una rete locale wireless (WLAN) e consentire l'accesso a Internet ai PC collegati (v. pag. 10).
- impostare una rete locale composta da componenti di rete via cavo e wireless (v. pag. 12).

Rete locale via cavo (Ethernet)

In un rete locale via cavo i PC comunicano tra loro mediante cavo Ethernet. Il Gigaset SE366 WLAN stabilisce in tal caso la connessione tra i PC che possono essere collegati alle quattro prese LAN Ethernet. I PC devono essere dotati di una porta di rete (Ethernet). I nuovi PC di norma sono dotati di questa porta. Nei vecchi PC è necessario installare una scheda di rete Ethernet. Il collegamento tra PC e porta Ethernet LAN del Gigaset SE366 WLAN viene stabilito mediante cavo Ethernet (CAT5). Un cavo è fornito in dotazione, per cavi Ethernet aggiuntivi rivolgersi al rivenditore specializzato.

Il Gigaset SE366 WLAN consente contemporaneamente a tutti i PC l'accesso a Internet.



Rete locale wireless (WLAN)

In una rete locale wireless (WLAN) tutti i PC sono collegati tra loro wireless. I PC devono essere dotati di un adattatore di rete wireless (adattatore WLAN), per es. un Gigaset PC Card 300 oppure un USB-Adapter 300.

Per le reti wireless si distinguono due tipi di modalità operative:

- Modalità infrastruttura
- Modalità ad hoc

Modalità infrastruttura

La modalità infrastruttura collega reti wireless e via cavo tra loro. Oltre alle stazioni mobili la modalità infrastruttura necessita di un punto di accesso, per es. il Gigaset SE366 WLAN. Nella modalità infrastruttura le stazioni comunicano tra loro in rete sempre attraverso questo punto di accesso. Ogni stazione che si desidera aggiungere alla rete wireless deve essere registrata al punto di accesso prima che sia possibile eseguire lo scambio di dati.

Il punto di accesso crea il collegamento tra le stazioni mobili della rete wireless e una LAN (Ethernet) via cavo oppure Internet. In questo caso viene definita come la funzione del router dell'apparecchio. Il router spedisce verso l'esterno pacchetti dati che non sono indirizzati alle stazioni della rete e inoltra i pacchetti dati provenienti "dall'esterno" alla stazione della rete corrispondente.

Con il Gigaset SE366 WLAN si collegano

- PC in rete wireless con Internet e
- PC in rete wireless con una rete Ethernet.

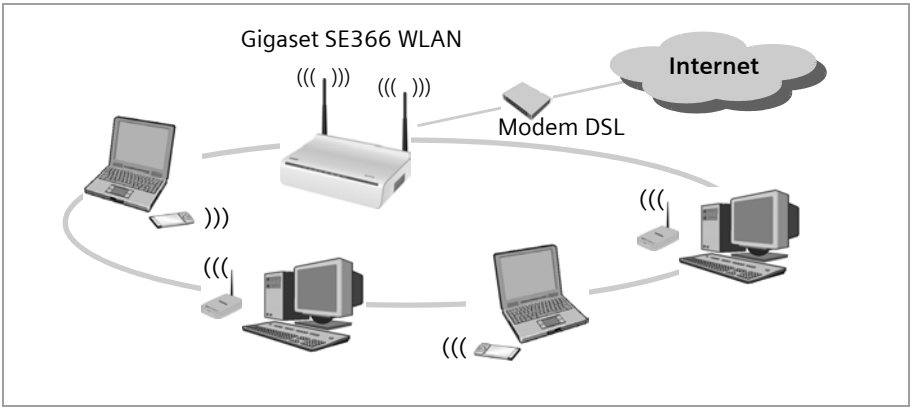
La modalità infrastruttura rappresenta la configurazione standard del Gigaset SE366 WLAN. Questa configurazione viene descritta nelle brevi istruzioni per l'uso allegate alla confezione.

Modalità ad hoc

Una rete ad hoc è una rete wireless impostata senza punto di accesso o router. I componenti di rete mobili che comunicano direttamente e in maniera wireless, creano la rete "ad hoc". Nella rete, tutte le stazioni hanno gli stessi diritti. Campi di applicazione per le reti ad-hoc sono presenti ovunque debbano essere realizzate reti di comunicazione veloci senza un'infrastruttura di rete esistente e dove i partecipanti sono mobili.

Collegare reti wireless con Internet

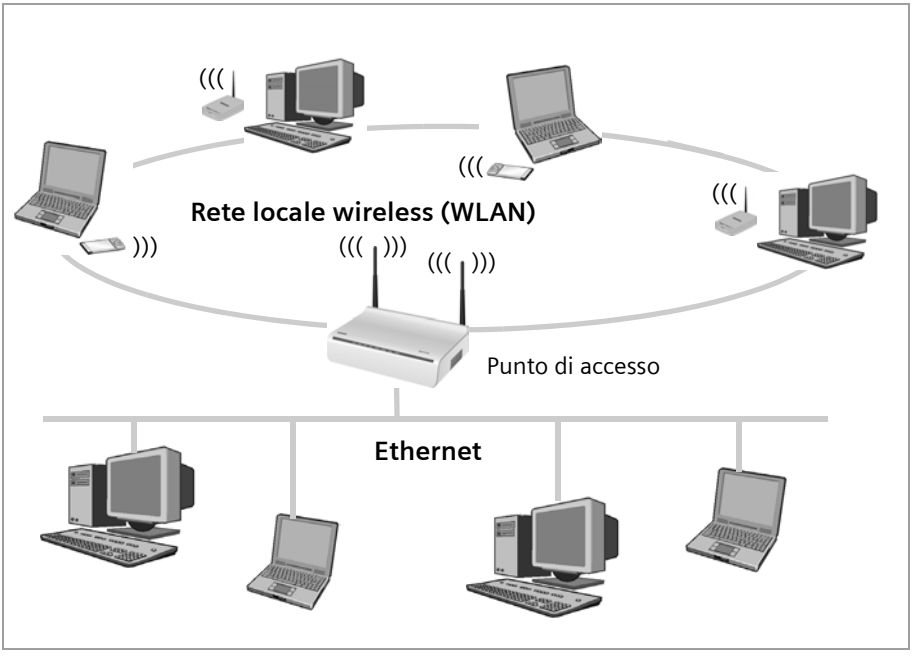
Il Gigaset SE366 WLAN consente tramite la sua porta WAN l'accesso contemporaneo a Internet di tutte le stazioni della propria rete locale. Per utilizzare questa funzione, è necessario disporre di una porta DSL oppure via cavo fornita da un Operatore di rete. L'operatore di rete di solito mette a disposizione la porta e anche il modem.



Nella figura viene visualizzato l'impiego più frequente. Nella modalità infrastruttura uno o più PC comunicano wireless con il Gigaset SE366 WLAN. Il Gigaset SE366 WLAN invia i dati tramite modem DSL oppure via cavo in Internet. I dati da Internet ritornano per la stessa via sul PC.

Collegamento della rete wireless (WLAN) con Ethernet (LAN)

Le reti wireless possono operare senza problemi con le reti Ethernet esistenti. Se si desidera aggiungere le stazioni mobili a una rete via cavo esistente, è necessario collegare tutte le stazioni mobili a una rete wireless in modalità infrastruttura.



Il Gigaset SE366 WLAN è dotato di quattro interfacce Ethernet (porte LAN). È possibile collegare a queste porte LAN direttamente fino a quattro PC.

Tutti i PC possono avere accesso a Internet tramite il Gigaset SE366 WLAN.

Avvertenza:

è possibile collegare a una porta LAN anche un router Ethernet per avere accesso a una rete Ethernet più grande. Se si desidera collegare la rete Gigaset WLAN alla rete esistente, è necessario tenere conto delle numerose impostazioni. Non è possibile mostrare un esempio che corrisponda a tutti gli impieghi. La configurazione corrispondente dovrà essere impostata di volta in volta. Si consiglia di far eseguire la configurazione di una rete di questo tipo da uno specialista.

Funzioni di sicurezza

È possibile impedire mediante diversi metodi di crittografia e di autenticazione (WPA2/WPA-PSK,WPA2/WPA, WEP, controllo accesso MAC) l'accesso non autorizzato alla propria LAN wireless ovvero rendere illeggibili i dati ai non autorizzati. Le funzioni di sicurezza disponibili dipendono dalle componenti utilizzati nella rete locale. Ulteriori informazioni sull'installazione si trovano nel capitolo “Impostazione delle funzioni di protezione per rete wireless“ a pagina 38.

WPS

Wi-Fi Protected Setup (WPS) facilita la realizzazione di una rete wireless. Con esso non è più necessario configurare e armonizzare a mano i componenti tra loro.

Una rete wireless ha un nome (SSID) e per motivi di sicurezza richiede la crittografia del traffico di dati. Prima di permettere l'accesso di un adattatore WLAN ai propri servizi, il punto di accesso richiede un'autenticazione con SSID e, se la crittografia è attivata, chiave.

WPS utilizza il metodo di crittografia WPA-PSK o WPA2-PSK. Gli apparecchi dotati di WPS possono generare automaticamente un SSID e una chiave WPA (Pre-Shared Key, vedi sopra) e sincronizzarsi tra loro.

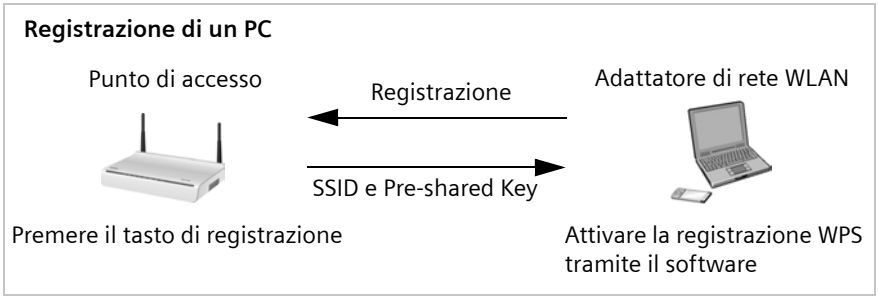
WPS non è possibile nelle reti nelle quali si usa il metodo di crittografia WEP o quello di autenticazione WPA2/WPA.

WPS offre due possibilità di registrazione:

- **con tasto di registrazione**

  Nell'Access Point (ad esempio nel Gigaset SE366 WLAN) si trova un tasto WPS, negli apparecchi Gigaset il tasto contrassegnato con **Registrazione** si trova sul retro dell'apparecchio. Se si preme questo tasto, per due minuti l'apparecchio è pronto alla registrazione di un client WLAN (ripetitore o adattatore di rete wireless).

  Al primo azionamento del tasto WPS, l'apparecchio genera automaticamente un SSID e una Pre-Shared Key. Se entro due minuti un client attiva la propria registrazione WPS, le impostazioni di sicurezza vengono scambiate e viene stabilita una connessione. Ci si assicura che entro due minuti si possa sincronizzare **un** solo client.


Registrazione di un PC
Punto di accesso
Registrazione
Adattatore di rete WLAN
SSID e Pre-shared Key
Premere il tasto di registrazione
Attivare la registrazione WPS tramite il software

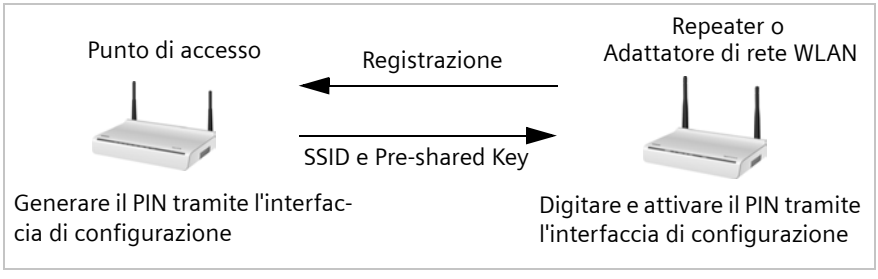
Nel Gigaset SE366 WLAN questa procedura è quella della modalità di registrazione ***Premere il pulsante*** (impostazione predefinita).

Notare che dopo il reset del Gigaset SE366 WLAN sulle impostazioni di fabbrica, alla prima pressione del tasto di registrazione vengono generati un nuovo SSID e una nuova Pre-shared Key con conseguente necessità di rieffettuare la registrazione dei client.

- Con Personal Identification Number (PIN)

  Il PIN rappresenta una elevata sicurezza di registrazione. Nessun altro apparecchio (ad esempio quello del vicino) può registrarsi senza che ciò venga notato. In un apparecchio WLAN, normalmente nell'Access Point, viene generato un PIN che va immesso negli altri client per la registrazione. Se un client si registra con questo PIN, i dati di sicurezza vengono sincronizzati.

  È anche possibile generare il PIN in uno dei client.


Punto di accesso
Registrazione
Repeater o
Adattatore di rete WLAN
SSID e Pre-shared Key
Generare il PIN tramite l'interfaccia di configurazione
Digitare e attivare il PIN tramite l'interfaccia di configurazione

Se nella rete si deve usare il PIN dell'apparecchio che si sta configurando, scegliere la modalità di registrazione ***Inviare il proprio PIN***.

Se l'apparecchio deve però usare il PIN di un altro apparecchio, scegliere la modalità di registrazione ***Digitare il PIN del dispositivo partner***.

Gli adattatori WLAN senza WPS possono essere ancora impostati manualmente, cioè SSID e chiave devono essere indicati a mano. La tecnica di crittografia usata deve essere WPA-PSK.

Prestazioni e possibilità d'impiego

Il Gigaset SE366 WLAN offre numerose caratteristiche e apre un ampio spettro di possibilità di applicazione, quali per esempio:

- **Internetaccesso**

  Il Gigaset SE366 WLAN consente a più utenti di accedere a Internet mediante la porta di un modem DSL o via cavo.

  – Poiché con molti operatori DSL l'accesso a Internet viene creato tramite il protocollo PPPoE, nel Gigaset SE366 WLAN è presente un Client PPPoE integrato, cioè non più è necessario impostare questo protocollo sul PC.

  – Accesso a Internet comune

    Se l'operatore di rete lo consente, il Gigaset SE366 WLAN supporta l'accesso a Internet per max. 252 utenti. In pratica, possono navigare più utenti nella rete allo stesso tempo utilizzando un solo account Internet.

- IP TV Streaming

  Il Gigaset SE366 WLAN permette la trasmissione senza fili di IP TV (televisione via Internet) al vostro ricevitore IP TV.

  Avvertenza:

  Notare però che, in funzione dei seguenti fattori, possono aversi disturbi nel Video-Streaming:

  – la rimozione di partner di comunicazione wireless,
  – la struttura dell'edificio (pareti, linee elettriche e condotte d'acqua),
  – altre sorgenti di disturbo (altri apparecchi WLAN, Bluetooth, microonde,...).

- **Creazione di una rete locale**

  Il Gigaset SE366 WLAN consente collegamenti

  – per quattro apparecchi tramite porte Ethernet con velocità di trasmissione di 10 oppure 100 Mbps (con riconoscimento automatico).

  – per massimo 32 periferiche mobili tramite interfaccia radio con velocità di trasmissione fino a 300 Mbit/s. Esso soddisfa lo standard IEEE 802.11n (Draft, vedi avvertenza in basso) e può interagire con tutti i prodotti che soddisfano lo standard IEEE 802.11 n, 802.11g o 802.11 b.

  Avvertenza:

  Lo standard di trasmissione IEEE 802.11n non è stata ancora rilasciato. Ciò avverrà probabilmente all'inizio del 2008. Dal punto di vista dell'hardware, il Gigaset SE366 WLAN è già predisposto per il nuovo standard di trasmissione. Se necessario, si potrà aggiornare il software dell'apparecchio (v. pag. 84).

L'utilizzo del Gigaset SE366 WLAN facilita la creazione di una rete in piccoli uffici oppure in ambito privato. Gli utenti possono scambiarsi dati oppure condividere diverse risorse nella rete, come per esempio un file server oppure una stampante.

- **Funzioni di sicurezza**

  Il Gigaset SE366 WLAN offre misure di protezione complete:

  – protezione Firewall contro accessi non autorizzati da Internet

    Tutti i PC della rete locale utilizzano per le connessioni Internet l'Indirizzo IP pubblico del Gigaset SE366 WLAN e quindi non sono visibili in Internet.
    Il Gigaset SE366 WLAN consente solo accessi da Internet originati dalla rete locale.

    Grazie al firewall il Gigaset SE366 WLAN offre inoltre protezione completa dagli attacchi degli hacker.

  – Filtro servizi e filtro URL

    Il Gigaset SE366 WLAN è in grado di filtrare l'accesso a Internet. Per questa ragione, si consiglia di stabilire quali PC devono utilizzare i servizi Internet.

    Inoltre è possibile disattivare l'accesso a determinati domini Internet e siti (filtro URL).

  – Controllo dell'accesso e crittografia per la rete locale wireless

    È possibile impedire mediante diversi metodi di crittografia e di autenticazione (controllo accesso WEP, WPA/WPA2-PSK,WPA/WPA2, MAC) l'accesso non autorizzato alla propria LAN wireless ovvero rendere illeggibili i dati ai non autorizzati. La funzione WPS permette di realizzare in modo veloce e semplice una connessione WLAN sicura.

  – La potenza di trasmissione può essere adattata alle condizioni locali. I tentativi di spionaggio alla rete locale vengono resi difficili se si limita la portata della rete radio solo quanto necessario.

- Ulteriori possibilità

  – Exposed Host

    È possibile impostare un PC collegato alla rete locale come server virtuale e renderlo visibile per gli accessi da Internet.

  – Port Forwarding

    In un PC della rete è possibile abilitare dei singoli servizi.

Procedimento per l'installazione e la configurazione

1. Installare dapprima una scheda di rete Ethernet oppure un Adattatore di rete wireless come per es. il Gigaset PC Card 300 oppure il Gigaset USB Adapter 300 nei PC che si desidera collegare al Gigaset SE366 WLAN. L'installazione è descritta nelle istruzioni d'uso dei relativi prodotti.

   Avvertenza:
   per l'installazione di adattatori di rete wireless: L'SSID standard del Gigaset SE366 WLAN è **ConnectionPoint**.

2. Eseguire i collegamenti necessari (PC, modem) al Gigaset SE366 WLAN e accendere l'apparecchio (vedere capitolo "Collegare il Gigaset SE366 WLAN" a pagina 22).
3. Prima che i PC possano comunicare con il Gigaset SE366 WLAN e tra loro in rete locale, è necessario modificare le impostazioni di rete adeguandole. Ciò è necessario normalmente quando si mantengono le impostazioni predefinite di Windows.

   Ulteriori informazioni su questo argomento si trovano nel documento „Configurare la rete locale" sul CD. Inizialmente collegare solo **un** PC e tramite questo eseguire la configurazione di base del Gigaset SE366 WLAN. Ulteriori PC possono essere collegati in seguito.

   Se si hanno client che supportano WPS (ad esempio adattatori di rete come il Gigaset PC Card 300), una connessione wireless può essere stabilita in modo molto semplice: Pressione del tasto di registrazione del Gigaset SE366 WLAN, l'attivazione della procedura di registrazione nel client. Ulteriori informazioni su questo argomento si trovano a pagina 23 e nelle istruzioni d'uso dell'adattatore di rete. La connessione con altri client e può essere stabilita anche a mano.
4. Configurare poi il Gigaset SE366 WLAN per mettere in funzione l'accesso a Internet dell'apparecchio (vedere capitolo "Impostazioni di base" a pagina 31). A tal fine sono necessari i dati di accesso dell'operatore di Rete.

Se si desidera utilizzare ulteriori funzioni del Gigaset SE366 WLAN, per es. le possibilità di protezione complete, utilizzare la procedura guidata per le impostazioni di protezione (v. pag. 35) oppure il menu ***Impostazioni avanzate*** (v. pag. 44).

Procedure iniziali

Contenuto della confezione

La confezione contiene quanto segue:

- un Gigaset SE366 WLAN,
- un alimentatore (100 V - 240 V / 12V DC 1A),
- un cavo con prese RJ45 (CAT5),
- un CD con diversi documenti (il manuale d'uso, Configurare la rete locale, garanzia) e il software per la scelta della lingua
- una guida rapida.

Requisiti del sistema

Per il funzionamento del Gigaset SE366 WLAN sono necessari:

- un computer con
  - un Adattatore di rete compatibile con IEEE 802.11n (Draft, vedi v. pag. 15), IEEE 802.11g o IEEE 802.11b.

    Avvertenze:
    la velocità massima di trasmissione dati per gli adattatori di rete compatibili 802.11n è di 300 Mbps, per gli adattatori compatibili 802.11g è di 54 Mbps e per gli adattatori di rete compatibili 802.11b è di 11 Mbps.

  Oppure

  - una porta Ethernet.
- un browser web per la configurazione del Gigaset SE366 WLAN (si consiglia il Microsoft Internet Explorer 6.0 o più recente, e Mozilla Firefox 1.0 o più recente),
- per l'accesso a Internet
  - un modem DSL oppure via cavo e uno splitter (per DSL),
  - i dati di accesso del proprio Operatore di rete.

Spie luminose e collegamenti

lato anteriore

Indicatori LED

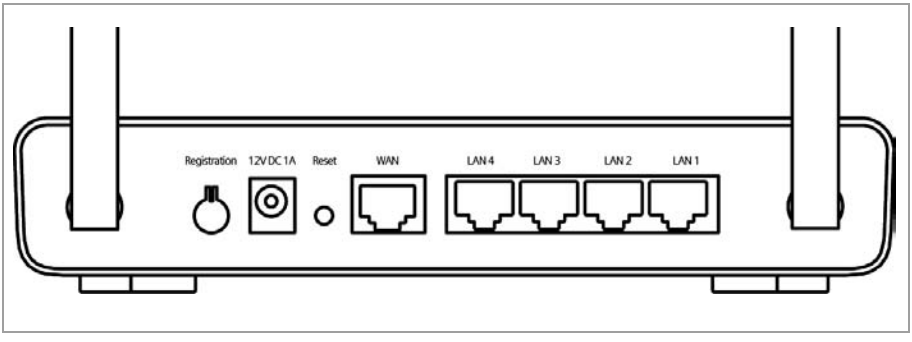
Sul lato anteriore dell'apparecchio si trovano LED che indicano lo stato operativo e facilitano l'installazione e la risoluzione dei problemi.

I LED indicano (da destra a sinistra) quanto segue:

LED	Stato	Stato
Power	Acceso	Il Gigaset SE366 WLAN è collegato alla rete elettrica.
	Spento	Il Gigaset SE366 WLAN non è collegato alla rete elettrica.
WAN	Acceso	Alla porta WAN è collegato un modem DSL.
	Lampeggia	Il collegamento WAN trasmette o riceve dati.
	Spento	Nessun modem collegato.
Online	Acceso	La connessione a Internet è stabilita (solo per la connessione a Internet tramite PPPoE e PPTP, v. pag. 45)
	Spento	Non esiste alcuna connessione a Internet.

LED	Stato	Stato
WLAN	**Nel funzionamento normale:**	
	Acceso	L'interfaccia radio è attivata, non c'è trasmissione dati.
	Lampeggia	Il Gigaset SE366 WLAN sta inviando o ricevendo dati tramite interfaccia radio.
	Spento	L'interfaccia radio è stata disattivata.
	Durante la registrazione WPS:	
	Un (300 s)	La registrazione WPS ha avuto successo.
	Lampeggia lentamente	Registrazione WPS in corso.
	Lampeggia rapidamente	Registrazione WPS fallita.
	Lampeggia velocemente ad intervalli	Più di un client ha tentato di registrarsi.
LAN1 – LAN4	Acceso	Alla corrispondente presa LAN è collegato un dispositivo.
	Lampeggia	Il relativo collegamento LAN trasmette o riceve dati (traffico).
	Spento	Nessun apparecchio collegato.

Lato posteriore



Sulla parte posteriore del Gigaset SE366 WLAN sono presenti le seguenti prese ed elementi di comando:

Elemento	Descrizione
Registrazione	Tasto per l'attivazione della funzione WPS. In tal modo è possibile stabilire rapidamente una connessione wireless sicura con i PC. **Avvertenza**: La funzione del tasto di registrazione è disponibile anche nell'interfaccia operativa dell'apparecchio (v. pag. 68). Il tasto di registrazione può essere disattivato proteggendolo così da usi impropri (v. pag. 86).

Elemento	Descrizione
12V DC 1A	Presa per l'alimentatore accluso. **Avviso**: un alimentatore diverso da quello fornito in dotazione potrebbe danneggiare il Gigaset SE366 WLAN.
WAN	Presa della porta da collegare al modem DSL.
LAN1 – LAN4	Quattro prese switch 10/100 Mbps con riconoscimento automatico della velocità (RJ-45). È possibile collegare fino a quattro apparecchi con porta Ethernet (ad es. PC, Hub oppure Switch).

Reset

Il tasto Reset si trova dietro una piccola apertura contrassegnata con **Reset**.

- Funzione di riavvio (reset del software): premere per più di 1 secondo e meno di 5 secondi il tasto per il riavvio dell'apparecchio. Tutte le operazioni di configurazione e le impostazioni restano invariate.
- Funzione di reset (ripristino delle impostazioni di fabbrica): Premere il pulsante per almeno 5 secondi per ripristinare le impostazioni di fabbrica.
  Avvertenza: tutte le operazioni di configurazione eseguite alla prima messa in funzione andranno perse. Ciò vale anche per i dati generati tramite WPS per la rete wireless (SSID e Pre-shared Key).
  Il nuovo firmware resta invariato.

Posizionamento del Gigaset SE366 WLAN

Il Gigaset SE366 WLAN può essere posizionato in qualsiasi luogo in ufficio o a casa. Non è necessario nessun cablaggio speciale. Tuttavia si consiglia di osservare le seguenti disposizioni:

- Installare l'apparecchio a distanza da sorgenti di calore, irradiazione solare diretta e altri apparecchi elettrici.
- Non posizionare l'apparecchio su una superficie sensibile al calore.
- Non collocare alcun oggetto sul apparecchio. Tutte le fessure di aerazione devono essere libere per la circolazione dell'aria.
- Posizionare l'apparecchio su un supporto antisdrucciolo.
- Posare i cavi in modo tale che nessuno possa inciamparvi.
- Nel luogo di installazione del Gigaset SE366 WLAN deve essere disponibile una presa adatta, oltre alla possibilità di collegamento all'interfaccia Ethernet di un PC o ad una rete cablata.
- Il luogo di installazione non deve trovarsi nelle immediate vicinanze di apparecchi stereo, televisori o apparecchi a microonde, ecc, altrimenti possono verificarsi delle interferenze.
- Nel caso di montaggio a parete: nell'eseguire i fori per i tasselli, prestare attenzione a non danneggiare tubi o conduttori presenti all'interno della parete.

Avvertenze per l'uso

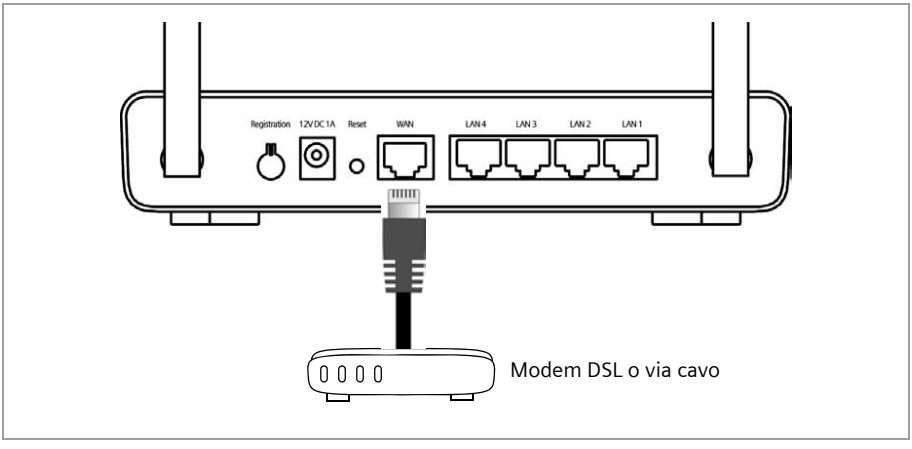
- Non aprire mai l'apparecchio o l'alimentatore. Per motivi di sicurezza elettrica, questi lavori devono essere effettuati da personale di servizio autorizzato.
- Non toccare mai i contatti di spinotti e prese con oggetti appuntiti o metallici.
- Non afferrare l'alimentatore con mani bagnate.
- Pulire l'apparecchio con un panno antistatico. Detergenti o solventi non sono adatti.

Collegare il Gigaset SE366 WLAN

Prima di iniziare a collegare i PC al Gigaset SE366 WLAN assicurarsi che nel PC sia presente un Adattatore di rete cablato o wireless. A tale proposito consultare le istruzioni per l'uso del prodotto. Nei PC più recenti o nei notebook gli adattatori Ethernet cablati e spesso anche wireless sono già montati dalla fabbrica.

Collegare al modem DSL o via cavo

➥ Collegare la presa contrassegnata con **WAN** sul retro del router e il proprio modem via cavo o DSL con un cavo Ethernet.



Avvertenza:

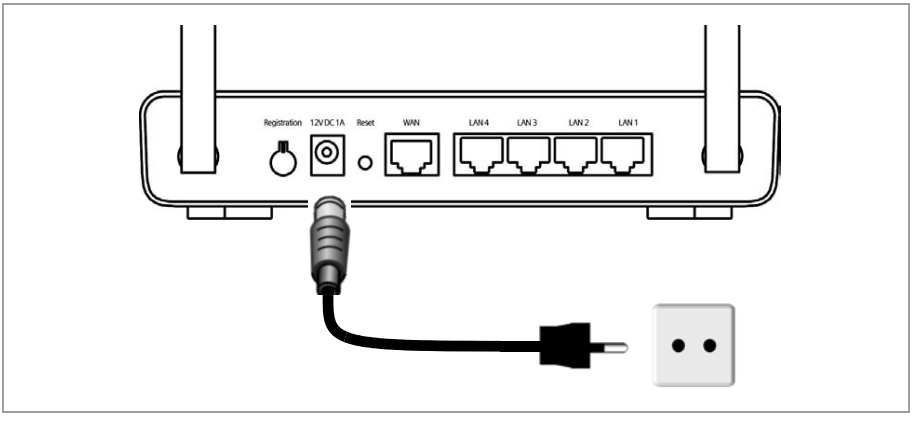
Per tutte le connessioni utilizzare un cavo Ethernet di categoria 5 con prese RJ-45 su entrambi i lati. Normalmente il cavo è compreso fra le parti fornite insieme al modem. Si può anche però usare il cavo giallo Ethernet accluso al Gigaset SE366 WLAN.

Collegare alla rete elettrica

Avvertenza:
Utilizzare esclusivamente l'alimentatore fornito con l'apparecchio (12V DC 1A).

➔ Inserire il cavo dell'alimentatore nella presa **12 V DC 1A** del Gigaset SE366 WLAN.

➔ Inserire l'alimentatore in una presa di corrente.



Collegare i PC wireless tramite WPS

Se si usa la funzione WPS, (v. pag. 13), è possibile stabilire la connessione wireless ad altri apparecchi WLAN facilmente tramite il tasto di registrazione.

➔ Premere almeno due secondi il tasto di registrazione sul retro dell'apparecchio per avviare la registrazione WPS.

➔ Attivare entro due minuti la registrazione WPS dell'Adattatore di rete wireless al PC. Il client ottiene i dati di sicurezza del Gigaset SE366 WLAN (SSID e Pre-shared-Key) ed è così registrato.

LED WLAN durante la registrazione WPS:

Un (300 s)	La registrazione WPS ha avuto successo.
Lampeggia lentamente	Registrazione WPS in corso.
Lampeggia rapidamente	Registrazione WPS fallita.
Lampeggia velocemente ad intervalli	Più di un client ha tentato di registrarsi.

Nella fase di registrazione può registrarsi un solo client. Se l'apparecchio con il LED WLAN mostra che più di un client ha tentato di registrarsi e che il client desiderato non è stato registrato con successo, un apparecchio estraneo si è allora eventualmente agganciato alla vostra WLAN. In questo caso bisognerebbe cambiare rapidamente la

chiave WPA-PSK a mano (v. pag. 69) ed eseguire la registrazione WPS dei client PIN (v. pag. 68).

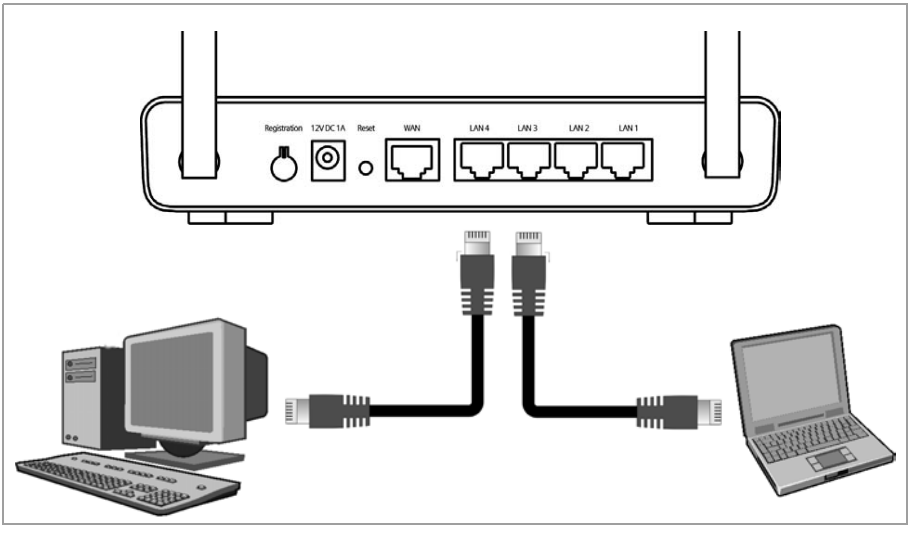
Ulteriori possibilità per la registrazione WPS sono descritte a pagina 68.

Collegamento cablato ad un PC

Se non si usa WPS, si consiglia di collegare prima l'apparecchio ad un PC tramite un cavo Ethernet. A seconda del tipo di utilizzo è necessario eseguire ancora alcune impostazioni tramite il programma di configurazione del Gigaset SE366 WLAN basato sul browser.

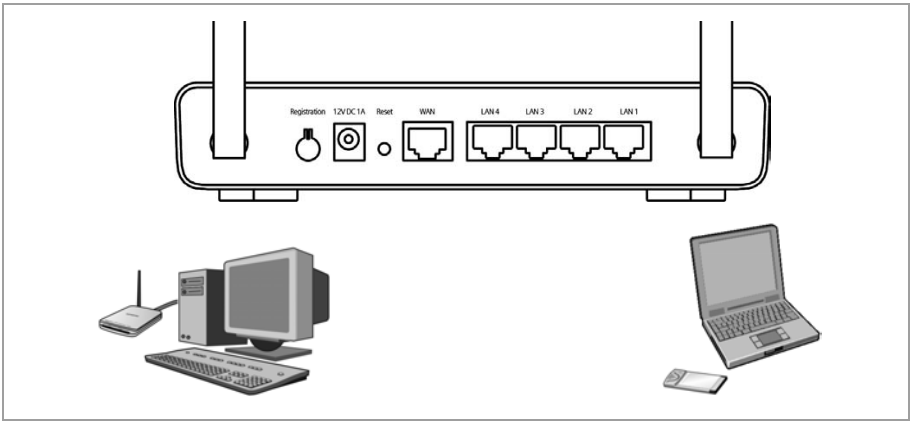
➞ Collegare una delle porte LAN gialle (**LAN1** – **LAN4**) nella parte posteriore del Gigaset SE366 WLAN e la porta Ethernet di un PC. Utilizzare un cavo Ethernet con prese RJ45. È possibile utilizzare anche il cavo Ethernet giallo in dotazione.

Le quattro porte LAN possono stabilire velocità di trasmissione automaticamente a 10 Mbps Ethernet oppure 100 Mbit/s Fast Ethernet e la modalità di trasmissione a Semiduplex oppure Duplex dipendentemente dalla prestazione dell'adattatore del proprio PC.



Collegare wireless ad un PC senza WPS

Per realizzare una connessione wireless si utilizza un adattatore di rete wireless, che deve essere installato nel computer. Può essere per es. un Gigaset PC Card 300,oppure un altro adattatoredi rete wireless compatibile con IEEE 802.11g o IEEE 802.11b.



Una Rete radio si definisce assegnando a tutti i dispositivi lo stesso SSID e impostando la stessa crittografia.

Assegnare agli adattatori di rete l'SSID del Gigaset SE366 WLAN. La preimpostazione dell'SSID è **ConnectionPoint**. Se all'adattatore di rete wireless dei computer è stato assegnato l'SSID corretto, la comunicazione radio viene istituita automaticamente quando il Gigaset SE366 WLAN viene collegato alla rete elettrica (v. pag. 25). Nel Gigaset SE366 WLAN e nell'nell'adattatore di rete wireless si dovrebbe poi impostare la crittografia.

Il Gigaset SE366 WLAN è ora pronto all'uso.

- L'indicatore LED **Power** sul lato anteriore è acceso.
- L'indicatore LED **WLAN** è acceso per segnalare che il Gigaset SE366 WLAN è pronto per stabilire connessioni wireless.

  Il collegamento radio verso un computer dotato di adattatore di rete wireless avviene ora automaticamente, purché l'adattatore di rete sia configurato con lo stesso SSID del Gigaset SE366 WLAN (v. pag. 25). Il collegamento radio può richiedere alcuni secondi. L'indicatore LED **WLAN** lampeggia quando tramite questo collegamento vengono inviati o ricevuti dati.
- Gli indicatori **LAN** si accendono quando alla presa LAN corrispondente è collegato un dispositivo tramite cavo Ethernet.

Per poter comunicare tramite Gigaset SE366 WLAN è necessario eseguire la configurazione di rete dei PC collegati. Di norma avviene automaticamente. A questo proposito leggere il documento „Das lokale Netzwerk konfigurieren“ sul CD.

L'interfaccia operativa

Dopo aver configurato le impostazioni di rete sul PC della propria rete, configurare ora il Gigaset SE366 WLAN sul PC mediante l'interfaccia operativa del Gigaset SE366 WLAN. È possibile eseguire la configurazione con un browser qualsiasi, si consiglia il Microsoft Internet Explorer 6.0 o superiore, Mozilla Firefox 1.0 o superiore.

Avvertenza:

Per poter avviare l'interfaccia di configurazione, può essere necessario disattivare il proxy http del browser (vedi pagina 93).

Se come browser si utilizza Mozilla Firefox oppure se si utilizza Internet Explorer con Windows XP Service Pack 2, è necessario configurare il blocco dei popup (vedere pagina 93).

Avvio dell'interfaccia operativa

Per accedere all'interfaccia operativa del Gigaset SE366 WLAN, operare nel modo seguente:

➥ Avviare il proprio browser.

➥ Digitare l'indirizzo IP del Gigaset SE366 WLAN nel campo indirizzi del browser.

`http://192.168.2.1`

Quando si richiama per la prima volta il programma di configurazione o si resetta l'apparecchio sulle impostazioni di fabbrica, viene avviato immediatamente l'assistente per le impostazioni di base (v. pag. 31).

In caso contrario compare la pagina di registrazione per l'immissione della password.

Viene visualizzata una pagina di login per l'inserimento della password.

➥ Digitare la password e cliccare su ***OK***.

Come standard al momento della consegna è preimpostata la password ***admin***.

Avvertenza:

Per motivi di sicurezza, in seguito la password deve essere modificata (v. pag. 35).

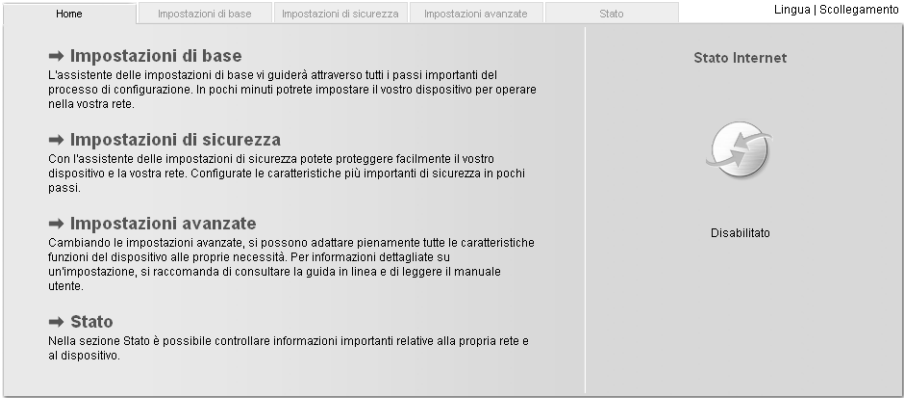
Viene visualizzata una pagina con le avvertenze di sicurezza.

➥ Cliccare su ***OK***.

Viene visualizzata la pagina iniziale.

La pagina iniziale

La pagina iniziale è il punto di partenza per tutte le attività di configurazione e di gestione dell'apparecchio.


Home
Impostazioni di base
Impostazioni di sicurezza
Impostazioni avanzate
Stato
Lingua | Scollegamento
➞ Impostazioni di base
L'assistente delle impostazioni di base vi guiderà attraverso tutti i passi importanti del processo di configurazione. In pochi minuti potrete impostare il vostro dispositivo per operare nella vostra rete.
➞ Impostazioni di sicurezza
Con l'assistente delle impostazioni di sicurezza potete proteggere facilmente il vostro dispositivo e la vostra rete. Configurate le caratteristiche più importanti di sicurezza in pochi passi.
➞ Impostazioni avanzate
Cambiando le impostazioni avanzate, si possono adattare pienamente tutte le caratteristiche funzioni del dispositivo alle proprie necessità. Per informazioni dettagliate su un'impostazione, si raccomanda di consultare la guida in linea e di leggere il manuale utente.
➞ Stato
Nella sezione Stato è possibile controllare informazioni importanti relative alla propria rete e al dispositivo.
Stato Internet
Disabilitato

Funzioni della pagina iniziale

Nella pagina iniziale è possibile

- scegliere la lingua dell'interfaccia operativa (v. pag. 29)
- stabilire una connessione a Internet (v. pag. 77),
- richiamare la procedura guidata per la configurazione di base, vedi Impostazioni di base (v. pag. 31),
- richiamare la procedura guidata per le Impostazioni di sicurezza (v. pag. 35)
- richiamare il menu ***Impostazioni avanzate*** per ulteriori possibilità di configurazione, (v. pag. 44).
- richiamare il menu ***Stato*** per avere informazioni sullo stato del Gigaset SE366 WLAN (v. pag. 77),

La procedura guidata, il menu ***Impostazioni avanzate*** e le informazioni sullo stato possono essere richiamati da qualsiasi pagina del programma di configurazione tramite le schede sul margine superiore dell'interfaccia operativa.

Nel programma di configurazione sono disponibili le seguenti funzioni:

Impostazioni di base	Con la procedura guidata, eseguire le impostazioni necessarie per stabilire la connessione a Internet. Inserire, inoltre, i dati relativi alla propria area geografica. Per la descrizione, vedere pagina 31 e seguenti.
Impostazioni di sicurezza	Con la procedura guidata, è possibile adottare le misure contro accessi non autorizzati al proprio Gigaset SE366 WLAN e alla rete locale. È possibile utilizzare per es. una password e impostare la crittografia del traffico. Per la descrizione, vedere pagina 35 e seguenti. Per la protezione della rete, si consiglia di eseguire la procedura guidata.
Impostazioni avanzate	Nel menu ***Impostazioni avanzate*** vengono offerte le funzioni aggiuntive. Qui si possono salvare e ripristinare ad esempio i dati della propria configurazione, stabilire il controllo di accesso ai PC e altro ancora. Le operazioni di configurazione sono opzionali e possono essere eseguite in un secondo momento. Per la descrizione, vedere pagina 44 e seguenti.
Stato	Nel menu ***Stato*** è possibile reperire informazioni sulla configurazione e sullo stato del Gigaset SE366 WLAN. Per la descrizione, vedere pagina 87 e seguenti.
Stato Internet	È possibile vedere lo stato della connessione a Internet e stabilire una connessione manuale a Internet (vedere pagina 77).
Lingua	È possibile scegliere la lingua dell'interfaccia operativa (vedere pagina 29).

Scelta della lingua

L'interfaccia operativa è disponibile in diverse lingue. Alla prima configurazione o dopo un reset sulle impostazioni di fabbrica, l'interfaccia operativa compare in tedesco (se anche il browser è in tale lingua) o in inglese (per tutte le altre lingue).

➡ Fare clic su ***Lingua*** in alto a destra della pagina di avvio.

➡ Se si desidera modificare la lingua predefinita, scegliere dall'elenco la lingua desiderata.

➡ Fare clic su ***OK*** per copiare l'impostazione.

Se necessario, caricare i dati per la lingua desiderata. I file si trovano sul CD. Si possono inoltre scaricare altre lingue da Internet e salvarle sul PC. Seguire le avvertenze riportate nella pagine dell'interfaccia operativa.

L'apparecchio viene riavviato per rendere operative le modifiche. Confermare il riavvio nella finestra di dialogo.

Al termine della procedura viene visualizzata la pagina iniziale.

Elementi dell'interfaccia operativa

Le pagine web dell'interfaccia operativa contengono gli elementi seguenti:

Pulsanti *Scollegamento*

A destra dell'interfaccia operativa si trova sempre il pulsante ***Scollegamento***. Facendo clic su ***Scollegamento***, viene annullata la sessione e viene visualizzata la pagina di registrazione.

Guida

Facendo clic sul punto interrogativo, vengono visualizzate le spiegazioni sulla pagina corrente dell'interfaccia operativa.

Pulsanti e simboli della procedura guidata

Nella procedura guidata vengono visualizzati graficamente i passi già eseguiti.

Dopo aver eseguito una modifica nella configurazione su una pagina, attivare la nuova impostazione cliccando su ***Avanti >*** sulla pagina in basso. Con il pulsante ***< Indietro*** si torna al passo di configurazione precedente, mediante ***Annulla*** si torna alla pagina iniziale.

Pulsanti nel menu *Impostazioni avanzate*

OK	Applica le impostazioni dell'utente nella configurazione del Gigaset SE366 WLAN.
Annulla	Cancella tutte le voci eseguite su una pagina dall'ultima esecuzione di ***OK***. Alla prima configurazione dell'apparecchio il pulsante non è ancora disponibile.

A seconda della funzione, è possibile utilizzare ulteriori pulsanti Essi vengono descritti nel punto corrispondente.

Impostazioni di base

Le Impostazioni di base vengono eseguite gradualmente attraverso la configurazione generale del Gigaset SE366 WLAN Essa contiene le impostazioni della zona e dell'accesso a Internet di zona.

Con Gigaset SE366 WLAN viene stabilita la connessione Internet per tutti i PC collegati all'apparecchio. Per la configurazioni sono necessari i dati di accesso del proprio Operatore di rete. Si consiglia di tenerli a portata di mano.

Avvertenza:

la procedura guidata per le Impostazioni di base riconfigura le proprie impostazioni Internet eventualmente già eseguite. Non viene applicata alle impostazioni WLAN eLAN;

durante la configurazione i dati di accesso vengono salvati nel Gigaset SE366 WLAN. Qualora si consegni l'apparecchio ad altre persone o si effettui una sostituzione presso il rivenditore, è necessario resettare le impostazioni iniziali (v. pag. 83). In caso contrario persone non autorizzate potrebbero utilizzare i propri dati di accesso a Internet con il conseguente addebito dei relativi costi.

Alla prima configurazione la pagina iniziale delle ***Impostazioni di base*** viene visualizzata automaticamente.

➥ Se dopo la prima configurazione si intendono effettuare di nuovo le Impostazioni di base, scegliere la voce ***Impostazioni di base*** sulla pagina di avvio per avviare la configurazione.

➥ Cliccare su ***Avanti >***.

Opzioni regionali

In questa pagina, selezionare la località corrente per le impostazioni internazionali.

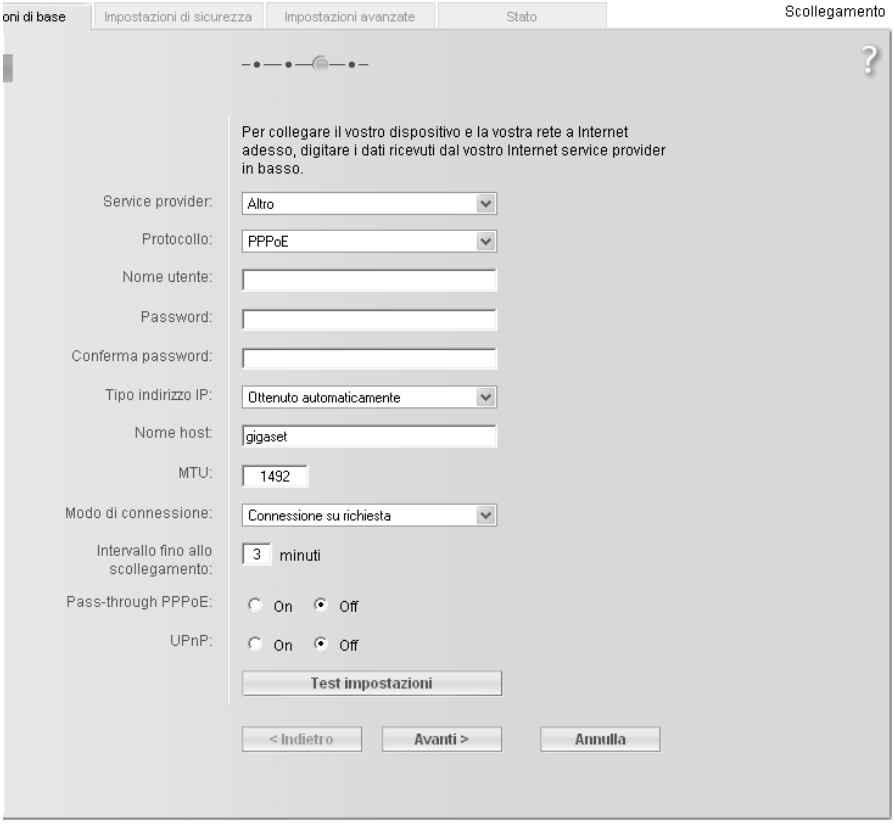
➥ Selezionare dall'elenco il Paese corrispondente. A seconda della scelta, è possibile eseguire le impostazioni per la conversione automatica dell'orario sull'ora legale e/o sul fuso orario.

➥ Selezionare l'opzione desiderata e/o scegliere il fuso orario della propria località.

➥ Cliccare su ***Avanti >***.

Configurazione della connessione a Internet

I dati di accesso necessari per la configurazione della connessione a Internet sono di norma contenute nella documentazione ricevuta del Operatore di rete (ISP).



➞ Selezionare l'Operatore di rete dal menu ***Service provider***. Qualora il proprio Operatore di rete non sia presente nell'elenco, scegliere l'opzione ***Altro***.

La lista offerta dipende dalla scelta del paese effettuata nella pagina ***Opzioni regionali***.

➞ Inserire i dati ricevuto dal proprio Operatore di rete.

Se se si sceglie il proprio operatore di rete dalla lista, la maggior parte dei dati necessari sono inseriti nella finestra come valori predefiniti.

Anche per l'opzione ***Altro*** si possono spesso effettuare delle impostazioni predefinite.

Controllare se il Protocollo è conforme ai dati del proprio operatore Internet.

Avvertenza:
la connessione a Internet è possibile solo dopo aver inserito correttamente tutti i dati
dell'Operatore di rete.

➥ Mediante il ***Modo di connessione*** scegliere le modalità delle sessioni Internet:

– Selezionare ***Sempre attivo*** se la connessione deve essere mantenuta in maniera permanente quando il Gigaset SE366 WLAN è acceso.

Avvertenza:
qualora si paghi una tariffa a tempo, questa opzione può comportare costi elevati di connessione.

– Selezionare ***Connessione su richiesta*** per stabilire automaticamente una connessione a Internet con applicazioni quali browser web o programmi e-mail.

– Indicare un intervallo di tempo nel campo ***Intervallo fino allo scollegamento*** allo scadere del quale la connessione a Internet viene automaticamente terminata in assenza di trasferimento dati (preimpostazione: 3 minuti, campo: da 1 a 99 minuti).

L'impostazione di questo tempo è valida solo per l'opzione ***Connessione su richiesta***. Una connessione duratura è possibile tramite l'opzione ***Sempre attivo***.

– Selezionare ***Connessione manuale*** per stabilire e terminare sempre la connessione a Internet in maniera manuale. Se si utilizza una tariffa a tempo, questa impostazione consente di risparmiare i costi di connessione. La connessione manuale viene descritta a pagina 82.

➥ Cliccare su ***Test impostazioni*** per verificare la connessione a Internet. L'apparecchio cercherà di stabilire una connessione a Internet. Verrà interrotta una eventuale precedente connessione a Internet.

Alla pagine ***Test connessione Internet*** sono disponibili le informazioni sui passi del test e sui risultati.

Pass-through PPPoE

Pass-through PPPoE consente l'utilizzo di una connessione a Internet aggiuntiva (con un Operatore di rete diverso) da un PC. Per ulteriori informazioni vedere pagina 47.

➥ Attivare ***Pass-through PPPoE*** se si desidera utilizzare questa funzione.

Utilizzo di UPnP (Universal Plug & Play)

I PC dotati di UPnP (Universal Plug & Play) offrono propri servizi di rete e utilizzano automaticamente i servizi offerti in rete. Per ulteriori informazioni vedere pagina 48.

➥ Attivare ***UPnP*** se si desidera utilizzare questa funzione.

➥ Cliccare su ***Avanti >***.

Riepilogo

Nella prossima sezione vengono visualizzate le impostazioni di base, eseguite con la procedura guidata, per la verifica.

➥ Per modificare le impostazioni, cliccare su. ***< Indietro***.

➥ Per confermare le impostazioni, cliccare su ***Fine*** per terminare la procedura guidata per le impostazioni di base.

Si accede automaticamente alla pagina iniziale delle ***Impostazioni di sicurezza***. Qualora si desideri eseguirle in un secondo momento, disattivare l'opzione ***Adesso voglio eseguire l'assistente per il setup della sicurezza.***.

Il Gigaset SE366 WLAN è ora configurato e pronto per stabilire una connessione a Internet.

Impostazioni di sicurezza

Le ***Impostazioni di sicurezza*** consentono impostazioni aggiuntive per migliorare la sicurezza della propria rete. È possibile

- immettere una Password per la configurazione del Gigaset SE366 WLAN (v. pag. 35),
- modificare l'identificazione della propria rete wireless (SSID) (v. pag. 37),
- impostare la Crittografia del traffico (v. pag. 38),
- limitare l'accesso alla propria rete wireless su determinati PC (v. pag. 42).

L'interfaccia operativa del Gigaset SE366 WLAN vi guida passo dopo passo attraverso la configurazione di protezione. Dopo aver completato una pagina, fare clic su. ***Avanti >***. Per modificare o verificare ancora i propri dati, fare clic su ***< Indietro***.

➥ Scegliere la voce ***Impostazioni di sicurezza*** nella pagina iniziale oppure nel registro per avviare la configurazione di sicurezza se, subito dopo le impostazioni di base, non è stato possibile arrivare alla pagina iniziale delle impostazioni di sicurezza.

➥ Per passare al passo successivo, fare clic su ***Avanti >***.

Avvertenze per l'uso di WPS

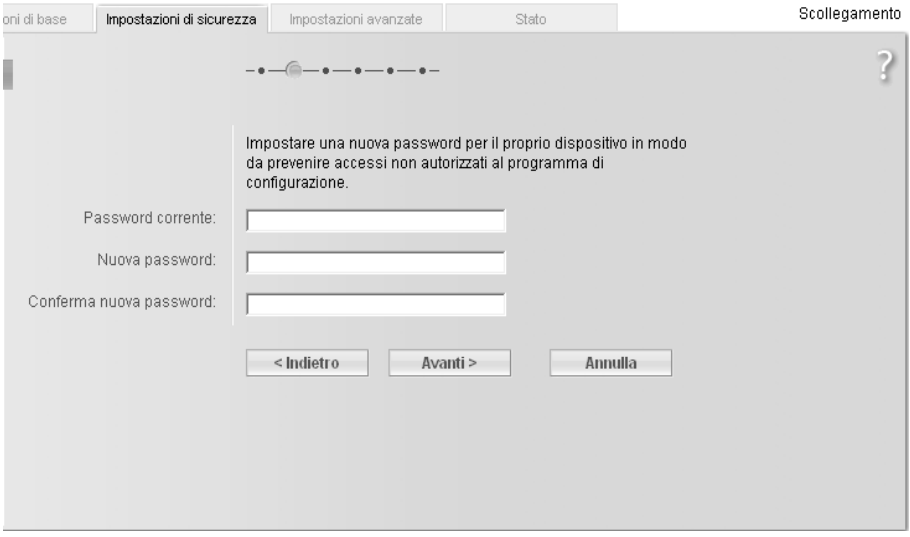
Il Gigaset SE366 WLAN è dotato di WPS (Wi-Fi Protected Setup). La sicurezza della propria rete wireless può essere così impostata con un solo clic (1 click only) (v. pag. 13).

Premendo il tasto di registrazione sul retro dell'apparecchio (v. pag. 20) vengono generati automaticamente un SSID e una chiave WPA-PSK (Pre-shared Key). I client che supportano WPS si possono così sincronizzare.

I dati impostati possono essere controllati nelle ***Impostazioni di sicurezza*** (vedi pagina 37 e pagina 39) o nelle impostazioni avanzate (v. pag. 69).

Cambiare la Password

Nel primo passo dell'assistente si può cambiare la password dell'interfaccia operativa. Al momento della consegna, la password del Gigaset SE366 WLAN è protetta con la Password ***admin***. Per evitare che persone non autorizzate possano eseguire modifiche alla configurazione, si consiglia di inserire una Password e di modificarla Password periodicamente.



➥ Digitare la password predefinita (o quella attuale già modificata) nel campo ***Password corrente***.

➥ Immettere una nuova password nel campo ***Nuova password*** e ripeterla nel campo ***Conferma nuova password***.

La Password può essere composta da 32 caratteri alfanumerici. Viene fatta distinzione tra caratteri maiuscoli e minuscoli. Non utilizzare nomi propri o concetti facilmente indovinabili. Mescolare lettere dell'alfabeto e numeri.

Avvertenza:

qualora si sia dimentica la propria Password, è necessario reimpostare il proprio Gigaset SE366 WLAN (v. pag. 20). È quindi di nuovo valida ***admin*** come Password. Tenere conto che in tal modo sono state reimpostate anche tutte le altre impostazioni di configurazione sulle impostazioni iniziali.

➥ Per passare al passo successivo, fare clic su ***Avanti >***.

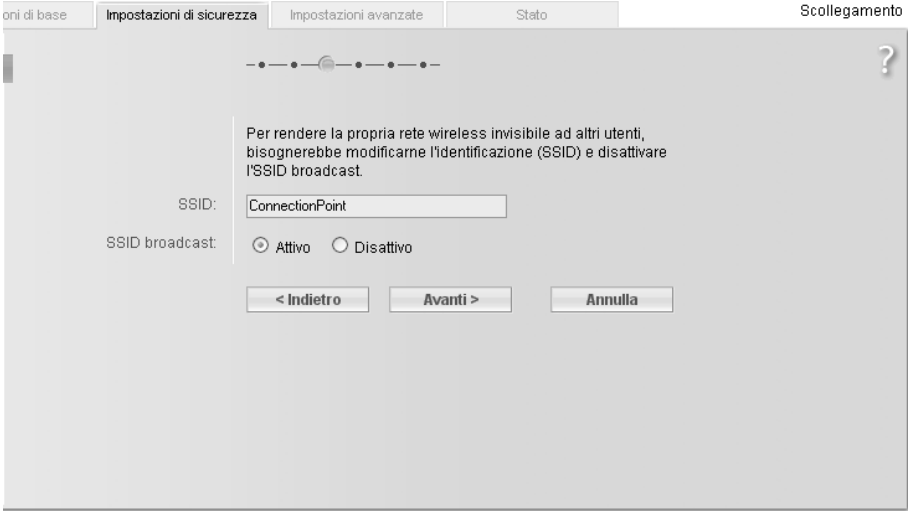
SSID

Per consentire la comunicazione tra i componenti di rete in collegamento wireless, è necessario che sia impostato in tutti lo stesso SSID (Service Set Identifier).

Al momento della consegna il Gigaset SE366 WLAN è dotato di SSID **ConnectionPoint**.

Avvertenza:

- Se si è già effettuata una registrazione WPS (v. pag. 68), in questa pagina si vede l'SSID generato. In questo caso l'SSID non va cambiato perché altrimenti sarà necessario rieffettuare la registrazione per tutti i client collegati e impostare prima il Gigaset SE366 WLAN sulle impostazioni di fabbrica.
- Se non si usa WPS, l'SSID andrebbe qui cambiato per motivi di sicurezza. Questa modifica va poi effettuata anche in tutti gli adattatori di rete wireless.



➞ Immettere nel campo ***SSID*** una stringa di propria scelta. Viene fatta distinzione tra caratteri maiuscoli e minuscoli. Essa può essere composta da 32 caratteri alfanumerici.

Annotarsi l'SSID. Esso è necessario per configurare gli adattatori di rete wireless.

Avvertenza:

la connessione agli adattatori di rete wireless viene interrotta fino a quando non viene immesso il nuovo SSID.

SSID broadcast

Se l'opzione è attivata (predefinita), il Gigaset SE366 WLAN invia l'SSID con tutte le trasmissioni di dati e l'SSID del Gigaset SE366 WLAN viene visualizzato sui PC dotati di adattatore di rete wireless. In questo caso è possibile che persone non autorizzate, in ascolto sulla rete, tramite l'SSID riescano ad accedervi.

➞ Selezionare l'opzione ***Disattivo*** per disattivare ***SSID broadcast***.

➞ Per passare al passo successivo, fare clic su ***Avanti >***.

Impostazione delle funzioni di protezione per rete wireless

Nel passo successivo è possibile impostare i metodi di crittografia e di autenticazione per la propria rete wireless.

Avvertenza:
Se sì è già effettuata una registrazione WPS, è allora impostata la crittografia WPA2-PSK/WPA-PSK. La seguente descrizione vale solo se non si utilizza WPS.

➞ Per passare al passo successivo, fare clic su ***Avanti >***.

Rispetto alle reti cablate, le reti wireless sono maggiormente esposte al pericolo di essere ascoltate. Con i normali adattatori di rete, un intruso ha bisogno soltanto di un apparecchio con adattatore WLAN (ad es. un Notebook oppure un PDA (Personal Digital Assistant)) con relativa scheda di rete configurata per ascoltare qualsiasi comunicazione tramite LAN wireless nelle vicinanze.

Il Gigaset SE366 WLAN imposta metodi efficaci di crittografia per evitare in larga misura l'ascolto non autorizzato.

È possibile utilizzare i seguenti meccanismi di protezione:

- WPA2-PSK oppure WPA2-PSK / WPA-PSK (vedere oltre)
- Crittografia WEP (Wired Equivalent Privacy, v. pag. 40)

Si consiglia di utilizzare WPA2-PSK se viene supportata da tutti i componenti della propria rete wireless.

Se si usa WPS, la crittografia WEP non viene supportata.

Nel menu ***Impostazioni avanzate*** sono disponibili ulteriori possibilità per l'impostazione della crittografia dei dati e dell'autenticazione (v. pag. 69).

WPA2 / WPA con Pre-shared Key (PSK)

WPA è un metodo più avanzato rispetto al WEP per la protezione delle reti wireless. Offre protezione elevata tramite chiave dinamica basata sul protocollo TKIP (Temporal Key Integration Protocol). Il nuovo standard WPA2 utilizza AES per la crittografia.

WPA-PSK è una modalità WPA speciale per l'utente privato e le piccole aziende senza server di autenticazione. Le chiavi di crittografia vengono create automaticamente con la Pre-shared Key e modificate automaticamente ("Rekeying") e dopo un lasso di tempo prestabilito vengono autenticate tra gli apparecchi in rete (Intervallo di rekey).

Ciascun PC (adattatore di rete) che accede a una rete wireless, protetta con WPA, deve a sua volta supportare il WPA. Per le modalità di utilizzo del WPA sul proprio PC, consultare le istruzioni d'uso dei propri adattatori di rete.

Se si è già effettuata la registrazione di un client con successo tramite WPS, su questa pagina si vede la Pre-shared Key generata. La Pre-shared Key può essere visualizzata in chiaro nelle impostazioni avanzate nella pagina ***Rete wireless*** – ***Crittografia***.

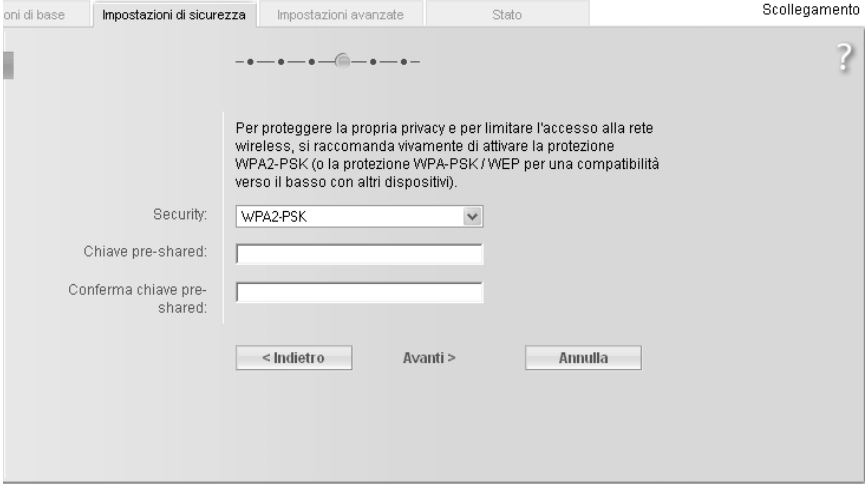
➥ Per passare al passo successivo, fare clic su ***Avanti >***.

Se non si usa WPS:

➥ Selezionare l'opzione***WPA2-PSK*** se viene supportata da tutti i componenti della propria rete wireless.

oppure

➥ Selezionare l'opzione ***WPA2-PSK / WPA-PSK*** se alcuni o tutti i componenti della propria rete wireless supportano il WPA con il protocollo TKIP.


oni di base
Impostazioni di sicurezza
Impostazioni avanzate
Stato
Scollegamento
Per proteggere la propria privacy e per limitare l'accesso alla rete wireless, si raccomanda vivamente di attivare la protezione WPA2-PSK (o la protezione WPA-PSK / WEP per una compatibilità verso il basso con altri dispositivi).
Security:
WPA2-PSK
Chiave pre-shared:
Conferma chiave pre-shared:
< Indietro
Avanti >
Annulla

➥ Immettere nel campo ***Chiave pre-shared*** una chiave a propria scelta (da 8 a max. 63 caratteri) e confermare con ulteriore immissione.

Avvertenza:

- è molto **importante** annotare la ***Chiave pre-shared***. Queste informazioni sono importanti per configurare in modo corretto l'adattatore di rete wireless;
- Dopo aver terminato le Impostazioni di sicurezza, è necessario modificare anche la crittografia negli adattatori wireless dei PC connessi poiché, in caso contrario, non sarà più possibile accedere alla rete wireless del Gigaset SE366 WLAN.

➞ Per passare al passo successivo, fare clic su ***Avanti >***.

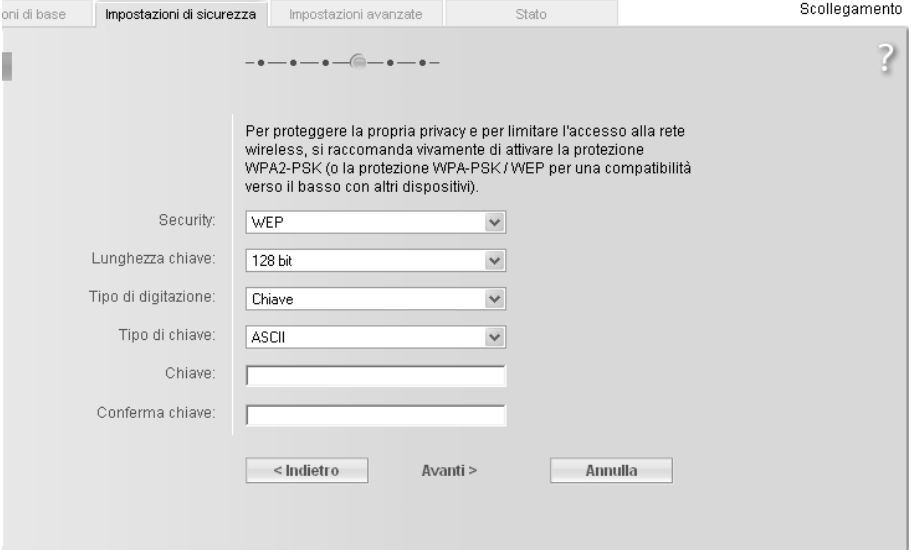
Crittografia WEP

WEP (Wired Equivalent Privacy) è un procedimento di crittografia per segnali radio in reti wireless basato sullo standard IEEE 802.11.

Quando si trasmettono dati wireless e non tutti i componenti della propria rete wireless supportano gli elevati standard di protezione WPA (v. pag. 39), si consiglia di attivare su questi componenti di rete la Crittografia WEP.

Se si è stabilita la connessione tramite WPS, non è la possibile utilizzare WEP.

Per applicare la crittografia è possibile scegliere tra la chiave standard a 64-Bit oppure la chiave più potente a 128-Bit. La chiave viene generata in formato esadecimale oppure in formato ASCII. È necessario utilizzare la stessa chiave per la crittografia e la decrittazione per il Gigaset SE366 WLAN e per tutti gli adattatori di rete wireless.



➞ Selezionare la ***Lunghezza chiave***: 64 oppure 128-Bit.

➞ Selezionare il ***Tipo di digitazione***, cioè se la chiave deve essere inserita manualmente o deve essere generata automaticamente attraverso una ***Passphrase***.

Inserimento manuale della chiave

➞ Selezionare il ***Tipo di chiave***, ***Hex*** oppure ***ASCII***.

Se si sceglie ***Hex***, è possibile utilizzare i numeri da **0** fino a **9** e le lettere da **A** fino a **F**.

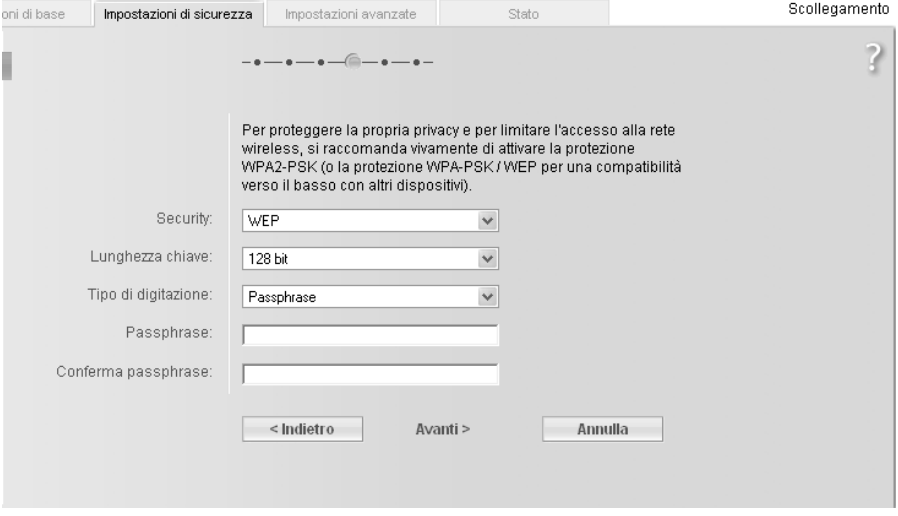
- Con una chiave a 64 Bit, la lunghezza è di 10 caratteri (esempio di una chiave valida: 1234567ABC).
- Con una chiave a 128 Bit, la lunghezza è di 26 caratteri (esempio di una chiave valida: 234567ABC8912345DEF1234567)

Se si sceglie***ASCII***, è possibile utilizzare i numeri da **0** fino a **9**, i caratteri da **A** fino a **Z** e da **a** fino a **z** e i caratteri speciali ASCII.

- Con una chiave a 64 Bit, la lunghezza è di 5 caratteri.
  Ecco qui un esempio di chiave valida: GIGA1
- Con una chiave a 128 Bit, la lunghezza è di 13 caratteri.
  Ecco qui un esempio di chiave valida: GIGASET_SE336

➞ Confermare la chiave con ulteriore immissione nel campo ***Conferma chiave***.

Generazione della chiave tramite Passphrase



➞ Immettere una ***Passphrase*** (fino a 32 caratteri) e confermare con ulteriore immissione. La chiave viene generata automaticamente.

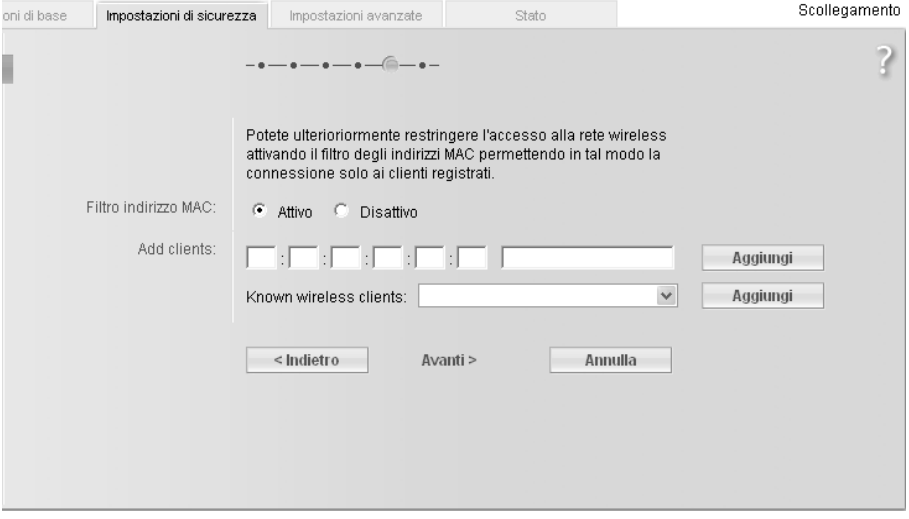
Avvertenza:

- è molto **importante** annotare la chiave ovvero la stringa. Queste informazioni sono importanti per configurare in modo corretto l'adattatore di rete wireless;
- Dopo aver terminato le Impostazioni di sicurezza, è necessario modificare anche la crittografia WEP negli adattatori dei PC poiché, in caso contrario, non sarà più possibile accedere alla rete wireless del Gigaset SE366 WLAN.

➞ Per passare al passo successivo delle Impostazioni di sicurezza, fare clic su ***Avanti >***.

Controllo di accesso nella rete wireless

In questo passo è possibile stabilire quali PC possono avere accesso wireless al Gigaset SE366 WLAN e, quindi, alla propria rete locale. Il controllo di accesso si basa sull'Indirizzo MAC degli adattatori di rete dei PC. È possibile immettere a mano gli indirizzi MAC dei PC oppure sceglierli dall'elenco dei PC già collegati.



Nei parametri iniziali il controllo di accesso è disattivato. Ciò significa che possono collegarsi tutti i PC che utilizzano il SSID corretto e la giusta crittografia.

➞ Selezionare accanto a ***Filtro indirizzo MAC*** l'opzione ***Attivo*** per attivare il filtro MAC.

Inserimento manuale degli indirizzi MAC

➞ Immettere gli indirizzi MAC dell'adattatore di rete. Gli indirizzi si trovano di solito nella parte inferiore dell'apparecchio su un adesivo.

➞ Inserire il nome del PC.

➞ Fare clic su ***Aggiungi*** per aggiungere la voce all'elenco.

Scelta dall'elenco dei PC collegati

➞ Selezionare il PC desiderato dall'elenco ***Client wireless noti***. Vengono visualizzati tutti i PC che sono al momento collegati con il router con l'SSID corretto.

➞ Fare clic su ***Aggiungi*** per aggiungere il PC selezionato all'elenco.

Avvertenze:

- Se si è attivato il controllo di accesso tramite i filtri MAC e si intende utilizzare WPS, notare che la registrazione sarà possibile solo a quei client registrati nella lista degli indirizzi MAC.
- quando si attiva il controllo di accesso MAC, è necessario immettere almeno il PC dal quale si configura il Gigaset SE366 WLAN. In caso contrario non sarà più possibile accedere all'interfaccia operativa e viene visualizzato il relativo messaggio di errore.
- Qualora per errore fosse stato negato a tutti i PC l'accesso al Gigaset SE366 WLAN sono disponibili due opzioni:
  - È possibile reimpostare completamente il Gigaset SE366 WLAN sulle impostazioni di fabbrica (v. pag. 20).
  - È possibile collegare un PC con connessione LAN (via cavo) al Gigaset SE366 WLAN. Poiché il controllo di accesso MAC è valido solo per i PC collegati "wireless", è possibile modificare la configurazione da questo PC.

➞ Per passare al passo successivo, fare clic su ***Avanti >***.

Salvataggio delle impostazioni

Nella pagina successiva, completare la procedura guidata e salvare le impostazioni. Tenere conto dei rischi di protezione esistenti in seguito.

➞ Fare clic su ***Fine*** per completare la procedura guidata.

Le impostazioni sono ora attive sul proprio Gigaset SE366 WLAN.

Avvertenza:

è ora possibile configurare, se impostata, la chiave WEP oppure WPA anche per l'adattatore di rete wireless del proprio PC. Successivamente è possibile collegarsi di nuovo wireless al proprio Gigaset SE366 WLAN.

Configurazione delle Impostazioni avanzate

Nel menu ***Impostazioni avanzate*** è possibile configurare tutte le opzioni del Gigaset SE366 WLAN. È possibile, se necessario, modificare anche le impostazioni eseguite con la procedura guidata. Nella tabella seguente sono riportate le possibilità del menu.

Menù	Descrizione
Internet	In questo menu sono comprese tutte le impostazioni riguardanti Internet. In particolare, è possibile ◆ verificare la configurazione dell'accesso a Internet e modificare (v. pag. 45) oppure stabilire un server DNS preferito (v. pag. 49) ◆ configurare il firewall, ovvero una serie di funzioni di protezione e funzioni speciali, per es. il controllo di accesso dei PC locali a Internet oppure il blocco di determinate pagine Internet (v. pag. 50), ◆ eseguire le necessarie impostazioni NAT per fornire alcuni servizi in Internet (v. pag. 56), ◆ impostare il DNS dinamico per un indirizzo Internet statico del proprio apparecchio (v. pag. 61), ◆ configurare Quality of Service (v. pag. 62).
Rete locale	Qui è possibile modificare gli Indirizzo IP privato del Gigaset SE366 WLAN ed eseguire le impostazioni sul server DHCP (v. pag. 63)
Rete wireless	Qui è possibile effettuare le impostazioni per WPS e configurare le opzioni per la comunicazione wireless (SSID e crittografia) e limitare l'accesso al Gigaset SE366 WLAN (v. pag. 45). Si può inoltre ottimizzare la qualità di trasmissione nella WLAN e adattarla alle proprie esigenze (raggio di azione, velocità) (v. pag. 67).
Amministrazione	Qui è possibile eseguire o modificare diverse impostazioni di sistema, per es. immettere una password (v. pag. 79), impostare l'orario (v. pag. 78) oppure attivare la gestione remota (v. pag. 80). È inoltre possibile salvare i dati del proprio Gigaset SE366 WLAN oppure caricare nuovo firmware (v. pag. 82).

Configurazione della connessione Internet

Quando si configura il proprio Gigaset SE366 WLAN con entrambe le procedure guidate, viene configurata anche la porta WAN (accesso Internet). È possibile verificare o modificare queste impostazioni nel menu ***Internet***.

Questo menu offre, inoltre, molteplici possibilità per le impostazioni di protezione e le limitazioni di accesso a Internet nonché per la fornitura di alcuni servizi in Internet.

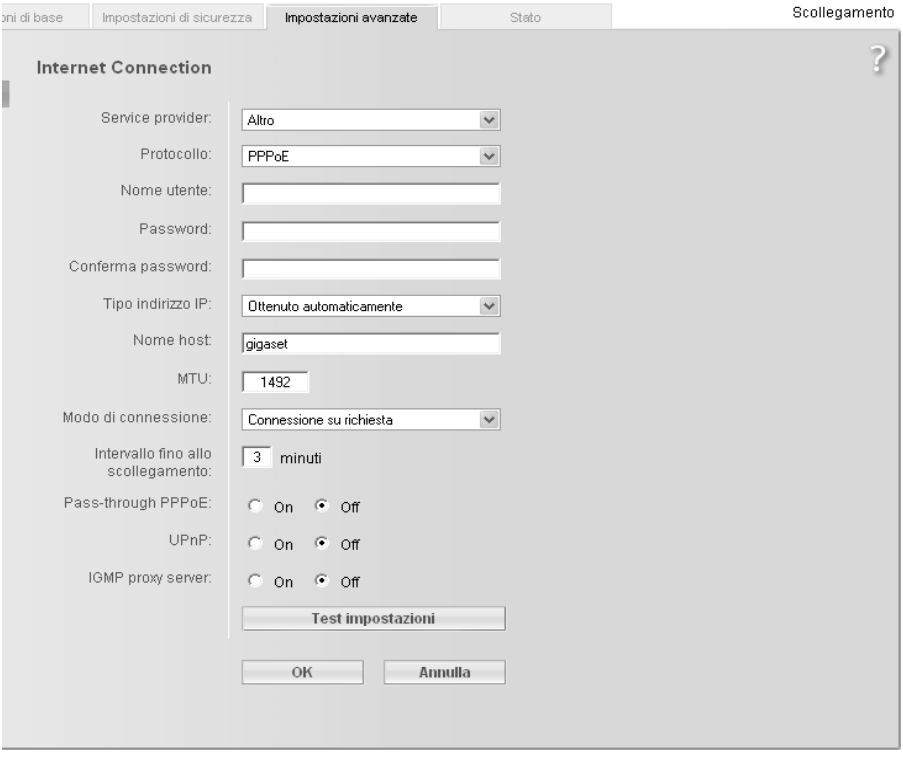
Internet

A pagina ***Internet*** si può permettere o impedire l'accesso a Internet attraverso il Gigaset SE366 WLAN.

Connessione Internet

In questa pagina è possibile impostare o modificare la configurazione della propria porta Internet. Le impostazioni eseguite devono corrispondere alle capacità fornite dall'Operatore di rete. Dati sbagliati possono causare danni al funzionamento di Internet.

➥ Se si desidera impostare o modificare le impostazioni per la connessione Internet, nel menu ***Impostazioni avanzate*** – ***Internet*** selezionare la voce ***Connessione Internet***.



➞ Selezionare l'operatore di rete dall'elenco ***Service provider***.

La lista di operatori di rete offerta dipende dalla scelta del paese effettuata nella pagina ***Opzioni regionali***.

➞ Inserire i dati ricevuti dal proprio ***Service provider*** nei campi corrispondenti.

Se se si sceglie il proprio operatore di rete dalla lista, la maggior parte dei dati necessari sono inseriti nella finestra come valori predefiniti.

Anche per l'opzione ***Altro*** si possono spesso effettuare delle impostazioni predefinite.

Controllare se il Protocollo è conforme ai dati del proprio operatore Internet.

Avvertenza:

per una configurazione corretta delle connessioni a Internet, tutti i campi devono completati in corrispondenza di dati del proprio Operatore di rete.

➥ Mediante il ***Modo di connessione*** scegliere le modalità delle sessioni Internet:

– Selezionare ***Sempre attivo*** se la connessione deve essere mantenuta in maniera permanente quando il Gigaset SE366 WLAN è acceso.

> **Avvertenza:**
> qualora si paghi una tariffa a tempo, questa opzione può comportare costi elevati di connessione.

– Selezionare ***Connessione su richiesta*** per stabilire automaticamente una connessione a Internet con applicazioni quali browser web o programmi e-mail.

– Indicare un intervallo di tempo nel campo ***Intervallo fino allo scollegamento*** allo scadere del quale la connessione a Internet viene automaticamente terminata in assenza di trasferimento dati (preimpostazione: 3 minuti, campo: da 1 a 99 minuti).

L'impostazione di questo tempo è valida solo per l'opzione ***Connessione su richiesta***. Una connessione duratura è possibile tramite l'opzione ***Sempre attivo***.

– Selezionare ***Connessione manuale*** se si desidera stabilire e terminare la connessione a Internet sempre in modalità manuale. Se si utilizza una tariffa a tempo, questa impostazione consente di risparmiare i costi di connessione. La connessione manuale viene descritta a pagina 77.

➥ Fare clic su ***Test impostazioni*** per verificare la connessione a Internet. L'apparecchio cercherà di stabilire una connessione a Internet. Verrà interrotta una eventuale precedente connessione a Internet.

Vengono visualizzate le informazioni relative alle operazioni del test eseguite con i risultati.

Si viene infine nuovamente reindirizzati alla pagina ***Connessione Internet***. Ora è possibile, eventualmente, correggere i propri inserimenti.

➥ Quando il test è positivo, fare clic su ***OK*** per copiare le impostazioni.

Pass-through PPPoE

Quando viene attivata la funzione ***Pass-through PPPoE***, un PC in rete può stabilire una connessione Internet tramite un proprio indicatore porta. Il router esegue queste connessioni.

➥ Scegliere nel menu ***Impostazioni avanzate*** – ***Internet*** la voce ***Connessione Internet***.

➥ Selezionare l'opzione ***Attivo*** per attivare ***Pass-through PPPoE***.

➥ Per accettare le impostazioni, fare clic su ***OK***.

Utilizzo di UPnP (Universal Plug & Play)

I PC dotati di UPnP (Universal Plug & Play) offrono propri servizi di rete e utilizzano automaticamente i servizi offerti in rete.

Avvertenza:

Verificare, eventualmente, se è installata la funzione UpnP nel sistema operativo del PC. Può essere necessario installare successivamente le componenti UPnP del proprio sistema operativo. Si consiglia di fare riferimento al manuale del sistema operativo del proprio PC.

Dopo aver installato la funzione UPnP nel sistema operativo di un PC e averle attivato nel router, le applicazioni su questo PC (ad. es. Microsoft Messenger) possono comunicare via Internet senza bisogno di espressa autorizzazione. In questo caso il router effettua automaticamente l'inoltro della porta (Port-Forwarding, v. pag. 59) e facilita quindi la comunicazione attraverso Internet.

Viene visualizzato un simbolo per il Gigaset SE366 WLAN nella barra delle applicazioni del PC su cui è installato UPnP. In Windows XP viene visualizzato il simbolo anche nelle connessioni di rete. Cliccando su questo simbolo si aprono direttamente le pagine di configurazione del Gigaset SE366 WLAN.

➡ Scegliere nel menu ***Impostazioni avanzate*** – ***Internet*** la voce ***Connessione Internet***.

➡ Attivare ***UPnP***.

Avvertenza:

con la funzione UpnP attivata le applicazioni del sistema possono allocare e utilizzare Porta su un PC. Ciò può costituire un rischio per la protezione.

➡ Fare clic su ***OK*** per confermare le impostazioni.

IGMP Proxy Server

IGMP (Internet Group Management Protocol) permette ad un PC di segnalare ad altri PC la propria appartenenza ad un gruppo Multicast. Con il multicasting un PC può inviare contenuto a diversi altri PC che hanno dimostrato interesse al contenuto del computer originale.

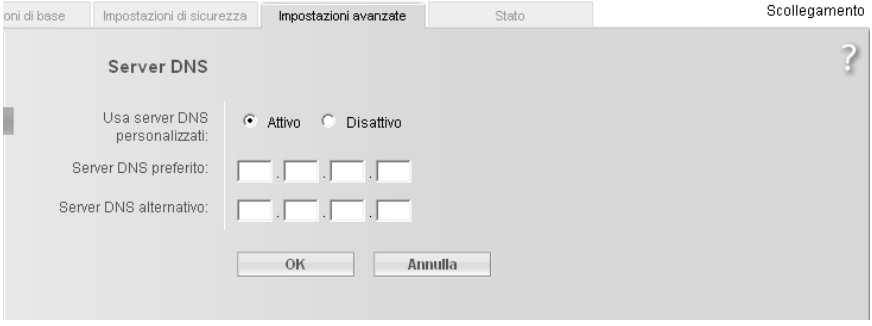
➡ Attivare ***Server proxy IGMP*** se si desidera utilizzare questa funzione.

Server DNS

Il DNS è un servizio decentrale che correla tra loro i nomi dei PC, gli indirizzi Internet (Nome di dominio). Per ciascun server o ciascuna LAN con porta Internet, il server DNS deve gestire queste informazioni.

In genere, l'Operatore di rete fornisce un Server DNS che esegue l'attribuzione se viene stabilita una connessione Internet. Se necessario, è possibile definire manualmente il server DNS da utilizzare per le connessioni Internet.

➥ Scegliere nel menu ***Impostazioni avanzate*** – ***Internet*** – ***Connessione Internet*** la voce ***Server DNS***.



➥ Attivare la funzione ***Usa server DNS personalizzati*** con l'opzione ***Attivo***.

➥ Immettere gli indirizzi IP del server DNS preferito (***Server DNS preferito*** e ***Server DNS alternativo***).

➥ Fare clic su ***OK*** per confermare le impostazioni.

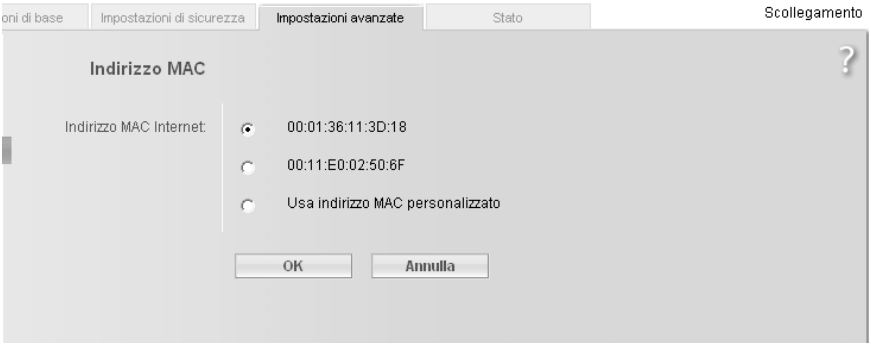
Indirizzo MAC

Se già prima della connessione del Gigaset SE366 WLAN si disponesse di accesso a Internet dello stesso operatore di rete, allora nella registrazione di questo accesso è possibile che sia stato utilizzato l'indirizzo MAC del proprio PC. In tal caso, sarebbe necessario sostituire l'indirizzo MAC corrente con l'indirizzo MAC registrato dall'Operatore di rete oppure farsi registrare dal proprio Operatore di rete un nuovo indirizzo MAC per proprio conto.

Procedere come segue:

➥ Collegare un PC al Gigaset SE366 WLAN e aprire l'interfaccia operativa.

➥ Nel menu ***Impostazioni avanzate*** – ***Internet*** – ***Connessione Internet*** selezionare la voce ***Indirizzo MAC***.



➥ Selezionare l'indirizzo MAC valido per la connessione Internet:

- ***Usa indirizzo MAC del dispositivo predefinito***: è possibile lasciare questo valore predefinito se viene utilizzato l'indirizzo MAC del Gigaset SE366 WLAN viene utilizzato per la connessione a Internet.
- ***Uso indirizzo MAC di questo PC***: selezionare questa opzione se l'indirizzo MAC del PC appena collegato è stato già registrato oppure se è stata eseguita una nuova registrazione dell'indirizzo MAC del PC su cui si sta lavorando.
- ***Usa indirizzo MAC personalizzato***: selezionare questa opzione se si è effettuata la registrazione di un nuovo indirizzo MAC tramite l'operatore di rete e questo non è l'indirizzo MAC del PC su cui si sta eseguendo la configurazione.

➥ Fare clic su ***OK*** per confermare le impostazioni.

Firewall

Le funzioni di firewall del Gigaset SE366 WLAN comprendono diverse funzioni di protezione per la propria rete locale.

È possibile:

- proteggere la propria rete dagli attacchi degli hacker (vedere oltre),
- bloccare l'accesso di un singolo PC ai servizi selezionati oppure a pagine Internet (v. pag. 53)

Le funzioni del firewall sono attivate e configurate alla consegna del Gigaset SE366 WLAN. Se si desidera disattivare il firewall, procedere come segue:

➥ Nel menu ***Impostazioni avanzate*** – ***Internet*** selezionare la voce ***Firewall***.

➥ Selezionare l'opzione desiderata.

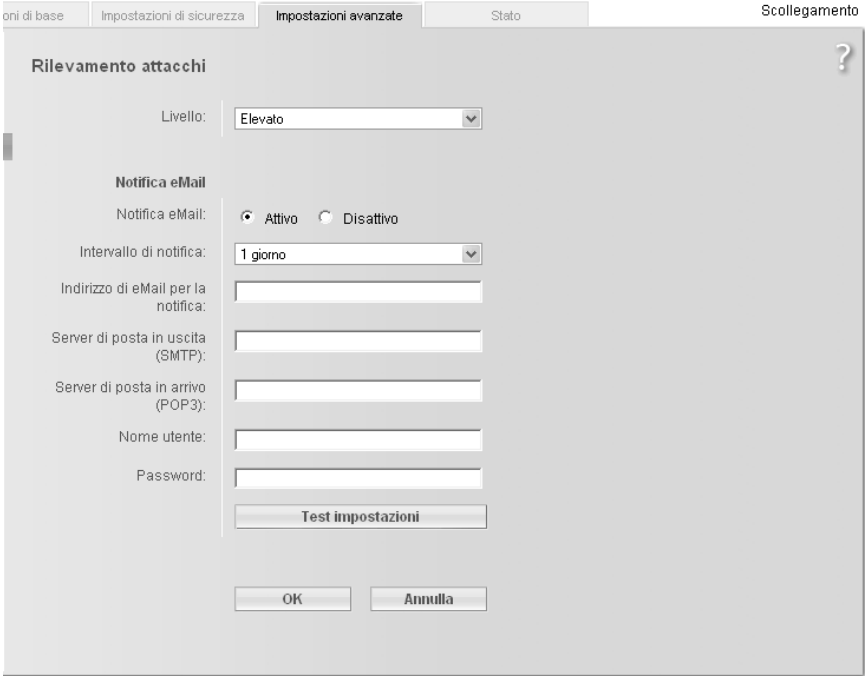
➥ Fare clic su ***OK*** per confermare le impostazioni.

Protezione dagli hacker

Se le funzioni del firewall del Gigaset SE366 WLAN sono attivate, l'apparecchio controlla e limita l'accesso del traffico in entrata tramite la porta DSL con una funzione denominata Stateful Packet Inspection (SPI). In tal modo il Gigaset SE366 WLAN è in grado di riconoscere e impedire determinati tipi di attacchi dalla rete come per es. Denial-of-Service (DoS). Gli attacchi DoS si dirigono contro apparecchi e reti con connessione a Internet. Lo scopo principale non è quello di rubare dati ma di indebolire l'apparecchio o la rete al punto da rendere inaccessibili le risorse di rete. Un tipico attacco degli hacker può essere costituito per es. da un PC estraneo che funge da apparecchio indebolito e riceve al suo posto i dati a questo inviati.

Con la funzioneRilevamento attacchi è possibile modificare le impostazioni standard del firewall e consentire di essere avvisati tramite e-mail del tentativo di attacco da parte di hacker.

➡ Nel menu ***Impostazioni avanzate*** – ***Internet*** – ***Firewall*** scegliere ***Rilevamento attacchi***.



➞ Selezionare il livello di protezione del firewall.

Il livello predefinito è ***Elevato*** e consente la massima protezione in caso di possibili funzioni limitate per applicazioni speciali.

- Il livello ***Medio*** combina un'elevata sicurezza con una bassa limitazione della funzionalità.
- Il livello ***Basso*** consente la massima funzionalità con possibile protezione ridotta.

Avviso via e-mail in caso di attacco di hacker

È possibile consentire di essere avvertiti via e-mail di un possibile attacco da parte di hacker.

➞ Nella finestra di dialogo immettere quanto segue:

- Selezionare ***Intervallo di notifica***, cioè con quale intervallo si desidera essere avvisati degli attacchi hacker. Qualora in passato un attacco hacker sia stato riconosciuto e respinto, si riceve ogni volta un riepilogo sull'evento.
- ***Indirizzo di eMail per la notifica***: immettere l'indirizzo e-mail a cui devono essere inviati gli avvisi.
- ***Server di posta in uscita (SMTP)***: immettere l'indirizzo del server della posta in uscita tramite il quale l'apparecchio può inviare gli avvisi.
- ***Server di posta in arrivo (POP3)***: qualora il server della posta in uscita richieda un'autenticazione tramite POP3 prima di inviare e-mail, immettere qui l'indirizzo del server della posta in entrata.
- Immettere il proprio ***Nome utenten*** e la corrispondente ***Password***.

➞ Fare clic su ***Test impostazioni*** per verificare i dati per gli avvisi e-mail.

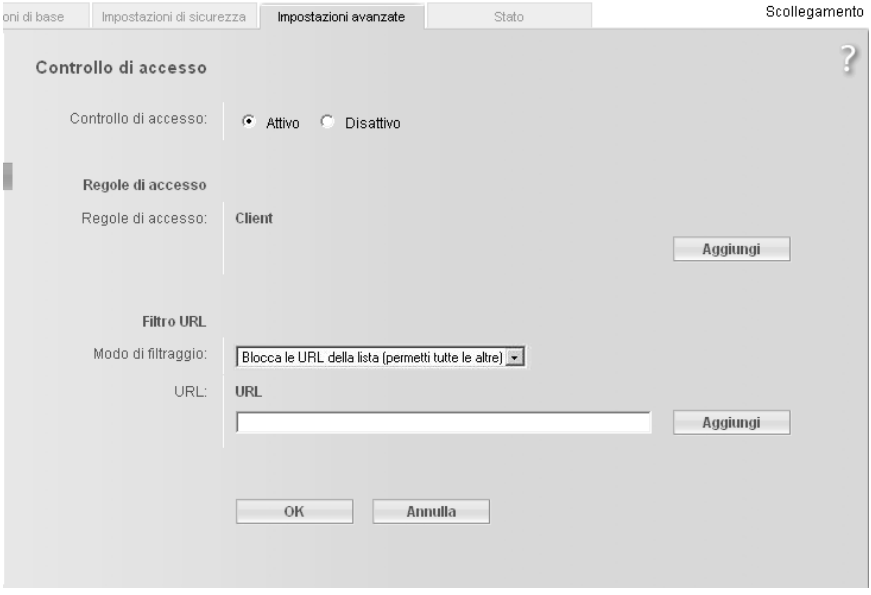
➞ Fare clic su ***OK*** per confermare le impostazioni.

Impostazione del controllo di accesso a Internet

La funzione***Controllo di accesso*** consente di bloccare l'attacco a diversi servizi Internet per uno o più PC.

➞ Scegliere nel menu ***Impostazioni avanzate*** la voce ***Controllo di accesso*** – ***Internet*** – ***Firewall***.

➞ Attivare la funzione ***Controllo di accesso*** con l'opzione ***Attivo***.

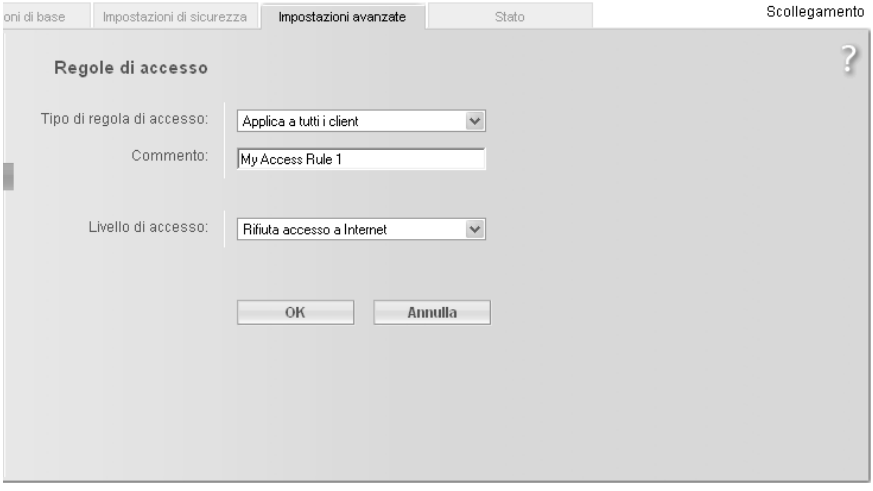


Sono disponibili diverse possibilità di impostazione per il ***Controllo di accesso***:

Regole di accesso

È possibile limitare l'attacco a Internet per tutti o determinati client della propria rete locale. È possibile permettere o bloccare l'accesso a URL e servizi.

➞ Fare clic su ***Modifica*** per creare una regola di accesso.



➞ Selezionare ***Tipo di regola di accesso*** dall'elenco:

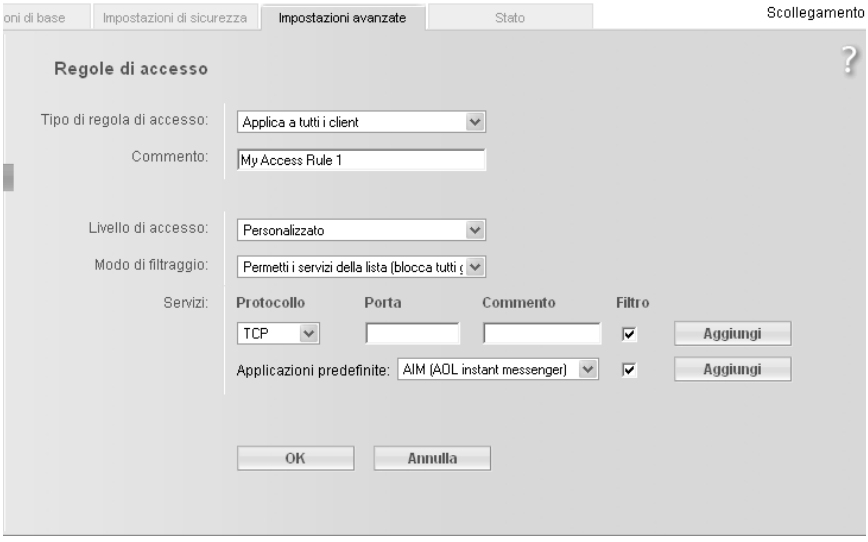
- ***Applica a tutti i client***: la regola vale per tutti i PC in rete.
- ***Specifica campo indirizzo IP***: selezionare i PC per i quali deve valere la regola attraverso l'informazione di un intervallo indirizzi IP.
- ***Specifica indirizzo IP*** oppure ***Specifica indirizzo MAC***: La regola vale per un PC selezionato tramite indirizzo IP o indirizzo MAC.

➞ Immettere un nome per la ***Descrizione*** della regola di accesso.

➞ Stabilire il ***Livello di accesso***.
È possibile ***Rifiuta accesso a Internet***, ***Permetti navigazione web con filtri URL***, ***Permetti navigazione web*** oppure eseguire le impostazioni definite dall'utente.

Se si sceglie l'opzione ***Permetti navigazione web con filtri URL***, si deve definire il filtro URL (v. pag. 56).

Se si sceglie ***Personalizzato***, si hanno le seguenti possibilità:



– Stabilire in ***Modo di filtraggio*** se i servizi selezionati devono essere consentiti o bloccati.
– Selezionare i ***Servizi*** che si desiderano consentire o bloccare.

  Selezionare il ***Protocollo*** e immettere la ***Porta*** corrispondente (un solo numero di porta, più numeri singoli di porta separati da virgole, intervalli porte costituiti da due numeri di porta separati da trattino o una combinazione qualsiasi di questi, per es. **`80,90-140,180`**). La ***Descrizione*** visualizzata consente l'identificazione di servizi diversi.
– Attivare l'opzione ***Filtro*** per utilizzare ciascun servizio per il filtro dei servizi.
– È possibile anche selezionare servizi dall'elenco ***Applicazioni predefinite***.
– Fare clic su ***Cancella*** per cancellare una voce. Cliccare su. Fare clic su ***Aggiungi*** per creare una nuova voce con i dati immessi o per l'applicazione selezionata predefinita.

➡ Fare clic su ***OK*** per confermare le impostazioni.

Filtro URL

Il filtro URL consente di bloccare l'accesso a determinate pagine Internet o domini Internet o di limitare l'accesso a determinate pagine Internet. Dopo aver immesso l'URL corrispondente, è possibile infine creare la regola di accesso che utilizza il filtro URL per i client selezionati nella rete.

➥ Nel menu ***Impostazioni avanzate*** – ***Internet*** – ***Firewall*** scegliere ***Controllo di accesso***.

➥ Selezionare il ***Modo di filtraggio***, cioè se si desidera consentire o bloccare l'accesso agli URL in elenco.

➥ Immettere l'URL desiderato nel campo.

➥ Fare clic su ***Cancella*** per cancellare una voce. Fare clic su ***Aggiungi*** per creare una nuova voce.

➥ Fare clic su ***OK*** per confermare le impostazioni.

Impostazione della funzione NAT

Il Gigaset SE366 WLAN è fornito con la funzione NAT (Network Address Translation). Scaricando gli indirizzi, diversi utenti della rete locale possono accedere a Internet tramite un solo indirizzo IP pubblico o più indirizzi IP pubblici. Nei parametri iniziali vengono scaricati tutti gli indirizzi IP locali negli indirizzi IP pubblici del router.

La funzione NAT ha la proprietà di non consentire a nessun dato da Internet di entrare nella rete locale a meno che sia esplicitamente richiesto da un PC della rete locale. Le principali applicazioni Internet funzionano senza problemi anche dietro il firewall NAT. Quando per es. si chiedono pagine Internet o si invia o si riceve un'e-mail, la richiesta di dati da Internet parte da un PC della rete locale e il router fa passare tali dati. Il router apre esattamente **una** porta per l'applicazione. Una porta è un indirizzo del PC interno attraverso cui è possibile scambiare dati tra un server in Internet e un client su un PC in rete locale. La comunicazione attraverso la porta avviene secondo le regole di un protocollo determinato (TCP o UDP).

Quando un'applicazione tenta da fuori di inviare una chiamata a un PC all'interno di una rete locale, il router non lo consente. Non esiste alcuna porta aperta su cui è possibile giungere ai dati nella rete locale.

Alcune applicazioni, quali i giochi in Internet, richiedono più connessioni, ciò significa più porte attraverso le quali i partecipanti non possono comunicare. Inoltre, per queste applicazioni deve essere consentito che le richieste dei partecipanti da Internet siano indirizzate ai partecipanti della rete locale. Queste applicazioni possono non funzionare se è attivata la funzione Network Address Translation (NAT).

Con la funzione Port-Forwarding (inoltro di richieste da determinate porte) si consente che il router inoltri le richiesta da Internet per un determinato servizio, per es. un gioco, alla porta corrispondente o alle porte su un PC su cui gira il gioco.

Port-Triggering è una variante specifica del Port-Forwarding. Diversamente dal Port-Forwarding il Gigaset SE366 WLAN in questo caso inoltra dati dell'intervallo porte al PC che ha inviato in precedenza i dati a Internet attraverso una determinata porta (Trigger-Port). In tal modo l'autorizzazione per la trasmissione dei dati è legata non a un PC specifico della rete ma soltanto ai numeri delle porte del servizio Internet desiderato.

Per la configurazione ciò significa:

- Viene stabilita per l'applicazione una cosiddetta Trigger-Port e il protocollo (TCP o UDP) che utilizza questa porta. Vengono allocate a questa Trigger-Port le porte pubbliche che devono essere aperte per l'applicazione.
- Il router verifica tutti i dati in uscita verso il numero di porta e il protocollo. Riconosce la corrispondenza della porta e del protocollo con una Trigger-Port definita, apre le porte pubbliche allocate e annota gli indirizzi IP del PC che ha inviato i dati. Nel caso in cui i dati da Internet tornino indietro attraverso queste porte pubbliche, rilascia questi dati e li inoltra al PC corretto. Un evento Trigger viene sempre da un PC all'interno della rete locale. Se una Trigger-Port viene interrogata dall'esterno, il router la ignora.

Avvertenza:

- un'applicazione configurata per il Port-Triggering può essere eseguita in un certo momento sempre soltanto da un partecipante in rete locale;
- fino a quando le porte pubbliche restano aperte possono essere utilizzate anche da persone non autorizzate per ottenere l'accesso a un PC della rete locale.

Alla consegna del Gigaset SE366 WLAN la funzione NAT (Network Address Translation) è attivata, cioè tutti gli indirizzi IP dei PC in rete locale con accesso a Internet vengono tradotti negli indirizzi IP pubblici.

Con le impostazioni NAT del Gigaset SE366 WLAN è possibile

- impostare il Port-Triggering per applicazioni speciali (v. pag. 58),
- impostare il Gigaset SE366 WLAN come server virtuale e configurare l'Inoltro porte (v. pag. 59),
- aprire il firewall per determinati PC (v. pag. 60).

Avvertenza:

nelle funzioni descritte di seguito è necessario stabilire che gli indirizzi IP dei PC non siano modificati. Quando gli indirizzi IP dei PC vengono immessi tramite server DHCP del Gigaset SE366 WLAN, per le impostazioni alla pagina ***Rete locale*** per il ***Tempo di lease*** è necessario selezionare l'opzione ***Non scade mai*** (v. pag. 64) oppure assegnare ai PC indirizzi IP statici.

È possibile attivare o disattivare la funzione NAT (valore predefinito: funzione NAT attivata).

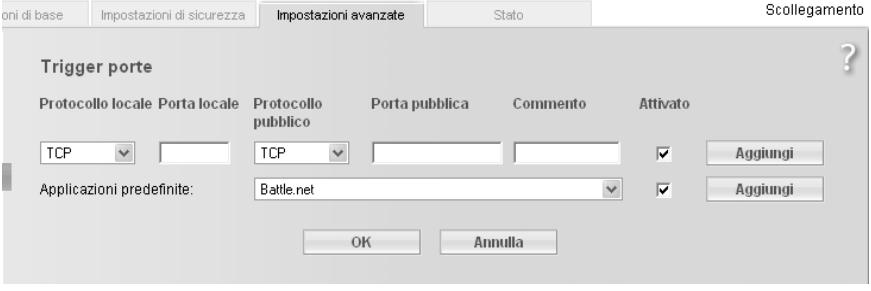
➞ Selezionare nel menu ***Impostazioni avanzate*** – ***Internet*** la voce ***Traslazione indirizzi (NAT)*** e selezionare l'opzione desiderata.

Port-Triggering

Quando si configura il Port-Triggering per una determinata applicazione, stabilire una cosiddetta Trigger-Port e il protocollo (TCP o UDP) che utilizza questa porta. Vengono allocate a questa Trigger-Port le porte pubbliche che devono essere aperte per l'applicazione.

È possibile, quindi, selezionare servizi Internet noti oppure fornire manualmente porte o intervalli di porte.

➞ Per impostare il Port-Triggering per un servizio, scegliere nel menu ***Traslazione indirizzi (NAT)*** la voce ***Trigger porte***.



➞ Selezionare dall'elenco ***Applicazioni predefinite*** quella desiderata.

➞ Fare clic sul pulsante ***Aggiungi***. I dati per il servizio desiderato vengono immessi nella pagina.

➞ Selezionare l'opzione nella colonna ***Attivato***.

Quando l'applicazione desiderata non è presente nell'elenco, è necessario immettere manualmente nella pagina i dati corrispondenti:

➞ ***Protocollo locale***: selezionare il protocollo da controllare per il traffico di dati in uscita.

➞ ***Porta locale***: immettere la porta da controllare per il traffico di dati in uscita.

➞ ***Protocollo pubblico***: selezionare il protocollo da autorizzare per il traffico di dati in entrata.

➞ ***Porta pubblica***: immettere la porta da aprire per il traffico di dati in entrata.

Avvertenza:
è possibile immettere un solo numero di porta, più numeri singoli di porta separati da virgole, intervalli porte costituiti da due numeri di porta separati da trattino o una combinazione qualsiasi di questi, per es. **`80,90-140,180`**).

- ***Descrizione***: immettere una descrizione utile per l'identificazione delle diverse voci.
- Selezionare l'opzione nella colonna ***Attivato***.
- Fare clic sul pulsante ***Cancella*** per cancellare una voce. Fare clic sul pulsante ***Aggiungi*** per aggiungere una nuova voce.
- Fare clic su ***OK*** per confermare le impostazioni.

Inoltro porte

Quando si configura Inoltro porte, il Gigaset SE366 WLAN si assume verso l'esterno il ruolo del server. Riceve le richieste di utenti remoti all'indirizzo IP pubblico e li inoltra automaticamente ai PC locali. Gli indirizzi IP privati dei server in rete locale restano protetti.

I servizi Internet vengono richiesti attraverso numeri di porta stabiliti. Per il redirect delle richieste di servizi al server che offre effettivamente il servizio, il Gigaset SE366 WLAN necessita di una tabella delle corrispondenze dei numeri delle porte. A tale scopo deve essere configurato il Inoltro porte.

- Per impostare il Port- Forwarding per un servizio, scegliere nel menu ***Traslazione indirizzi (NAT)*** la voce ***Inoltro porte***.

- Selezionare dall'elenco ***Applicazioni predefinite*** quella desiderata.
- Fare clic sul pulsante ***Aggiungi***. I dati per il servizio desiderato vengono immessi nella pagina.
- Selezionare l'opzione nella colonna ***Attivato***.

Quando l'applicazione desiderata non è presente nell'elenco, è necessario immettere manualmente nella pagina i dati corrispondenti:

➡ Selezionare dall'elenco ***Protocollo*** il protocollo del servizio fornito.

➡ Immettere in ***Porta pubblica*** il numero di porta del servizio fornito.

➡ Immettere nel campo ***Porta locale*** il numero di porta interno al quale devono essere inoltrate le richieste di servizi.

Avvertenza:
Si possono digitare un solo numero di porta o intervalli porte costituiti da due numeri di porta separati da trattino (ad esempio **`80`** o **`90-140`**).

➡ Immettere nel campo ***Indirizzo IP locale*** l'indirizzo IP del PC che fornisce il servizio.

Esempio: il server web stato configurato in modo da reagire alle richieste alla porta 8080. Le richieste di pagine web entrano, tuttavia, dalla porta 80 (valore predefinito). Quando si registra il PC nella tabella Forwarding e viene definita la porta 80 come porta pubblica e la porta 8080 come porta interna, tutte le richieste di servizio da Internet con numero di porta 80 vengono inoltrare al server web del PC che è stato definito con la porta 8080.

➡ Cliccare su ***Aggiungi***.

➡ Fare clic su ***Cancella*** se si desidera cancellare di nuovo i dati nella riga relativa.

➡ Selezionare l'opzione nella colonna ***Attivato***.

➡ Fare clic su ***OK*** per confermare le impostazioni.

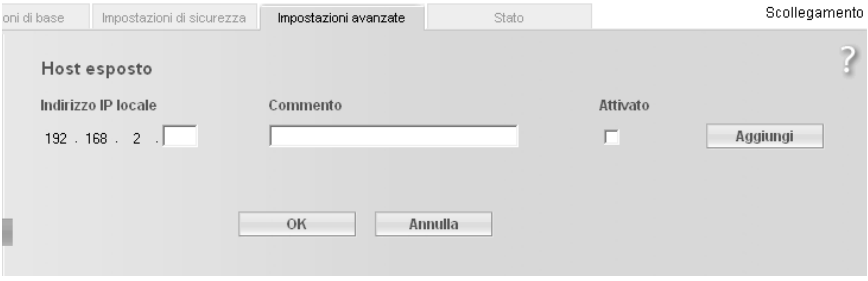
Apertura del firewall per determinati PC (Host esposto)

È possibile impostare nella propria rete locale un client come Exposed Host. L'apparecchio inoltra, quindi, a tale client tutto il traffico di dati in entrata da Internet. È possibile gestire, per esempio, il proprio server web su uno dei client in rete locale e renderlo accessibile per l'utente Internet.

Come Exposed Host il client locale è visibile direttamente in Internet e, quindi, esposto a rischi particolari (ad es. attacchi di hacker). Queste funzioni devono essere attivate soltanto se strettamente necessario (ad es. per la gestione di un server web) e le altre funzioni non sono sufficienti (ad es. Port-Forwarding). In tal caso è necessario adottare misure adeguate ai singoli client.

Avvertenza:
è possibile impostare soltanto un PC per ciascun indirizzo IP pubblico come Host esposto (vedere anche il capitolo "Inoltro porte" a pagina 59.

➡ Per impostare un PC come Host esposto, selezionare nel menu ***Traslazione indirizzi (NAT)*** la voce ***Host esposto***.



➞ Immettere l'***Indirizzo IP locale*** del PC da condividere come Host esposto.

➞ Immettere nel campo ***Commento*** un nome per il PC.

➞ Attivare la voce contrassegnando l'opzione.

➞ Fare clic su ***Aggiungi*** per aggiungere la voce all'elenco.

➞ Fare clic sul pulsante ***Cancella*** per cancellare la voce all'elenco.

➞ Fare clic su ***OK*** per confermare le impostazioni.

DNS dinamico

Un servizio che si mette a disposizione su Internet è accessibile tramite un Nome di dominio. A questo nome di dominio è connesso l' Indirizzo IP pubblico del proprio router. Se l'operatore di rete fornisce l'indirizzo IP per la porta WAN della rete locale dinamicamente, l'indirizzo IP del router può cambiare. Quindi l'attribuzione al nome del dominio non è più disponibile e il servizio non è più raggiungibile.

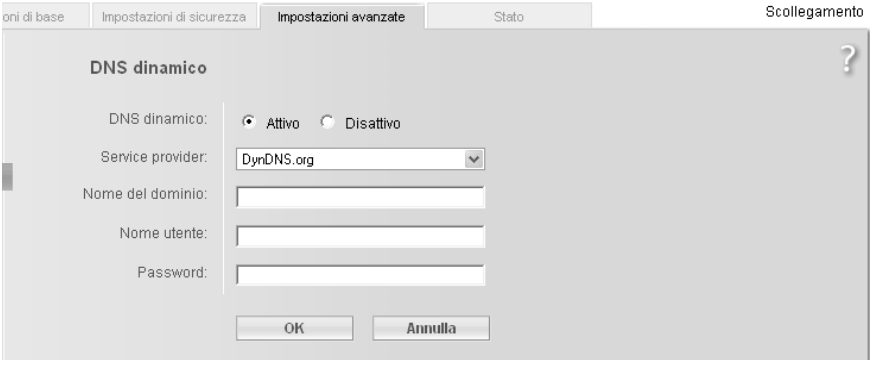
In questo caso occorre assicurarsi che l'assegnazione al nome del dominio venga aggiornato continuamente. Per questo serve il servizio DNS dinamico (DynDNS). Con il DynDNS è possibile assegnare al Gigaset SE366 WLAN un nome di dominio individuale e statico anche se non c'è un indirizzo IP statico.

Esistono in Internet diversi Operatori di rete che forniscono un servizio DynDNS gratuito. Il Gigaset SE366 WLAN utilizza il servizio DynDNS di **DynDNS.org** e di TZO.org. Se si usa il servizio di questi operatori di rete di DynDNS, il servizio è raggiungibile come sottodominio di uno dei domini di DynDNS.org in Internet.

Quando viene attivata la funzione DynDNS dell'apparecchio, questo controlla i propri indirizzi IP pubblici. Quando questo cambia, esso stabilisce una connessione alla pagina Internet e vi aggiorna l'indirizzo IP.

Avvertenza:
prima di utilizzare la funzione DynDNS del Gigaset SE366 WLAN, è necessario impostare un account presso l'operatore. Seguire le avvertenze riportate nella pagina Web dell'operatore. Digitare nella configurazione del routers i dati dell'utente.

➞ Per utilizzare la funzione DynDNS del router, selezionare nel menu ***Impostazioni avanzate*** – ***Internet*** la voce ***DNS dinamico***.



➞ Attivare la funzione ***DNS dinamico***.

➞ Selezionare dall'elenco ***Service provider*** il servizio che offre il DNS dinamico (DynDNS.org oppure TZO.com).

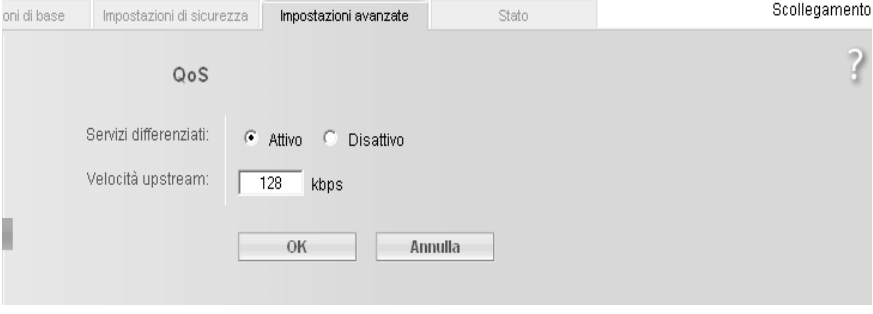
➞ Immettere ***Nome del dominio***, ***Nome utente*** e ***Password***. Le informazioni necessarie sono fornite al momento della registrazione dal ***Service provider***.

➞ Fare clic su ***OK*** per confermare le impostazioni.

QoS (Quality of Service)

Molte applicazioni di comunicazione e multimediali richiedono un'elevata velocità e una grande larghezza di banda per la trasmissione di dati tra la rete locale e Internet. Perciò, spesso, per numerose applicazioni è disponibile soltanto una connessione a Internet con capacità limitata. ***QoS*** (Quality of Service) suddivide questa capacità tra le diverse applicazioni e fornisce una trasmissione di dati immediata e continua mentre vengono trasmessi pacchetti di dati ad alta priorità in modo preferenziale.

➞ Nel menu ***Impostazioni avanzate*** – ***Internet*** selezionare la voce ***QoS***.



➥ Attivare la ***Servizi differenziati***, cioè la priorità di determinati servizi durante la trasmissione di dati tra la propria rete e Internet.

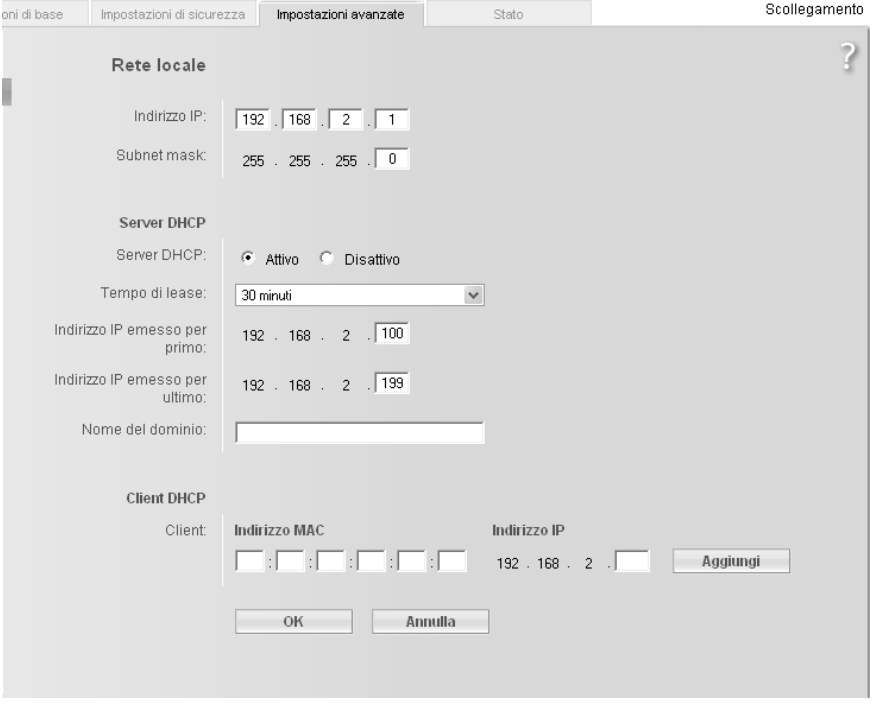
➥ Inserire nel campo accanto a ***Velocità upstream*** il valore massimo della propria linea DSL per la trasmissione dei dati in Internet. Il valore è stabilito nel contratto stipulato con l'operatore Internet.

➥ Fare clic su ***OK*** per confermare le modifiche.

Configurazione LAN

Con la configurazione LAN è possibile stabilire un Indirizzo IP per il Gigaset SE366 WLAN e configurare il server DHCP.

➥ Selezionare le ***Impostazioni avanzate*** – ***Rete locale***.



Stabilire l'indirizzi IP privato del Gigaset SE366 WLAN

In questa pagine è possibile modificare l'Indirizzo IP dell'apparecchio. L'indirizzo IP predefinito è 192.168.2.1. Si tratta dell'Indirizzo IP privato del Gigaset SE366 WLAN. Questo è l'indirizzo con cui è possibile raggiungere l'apparecchio nella rete locale. Questo indirizzo può essere utilizzato liberamente dal campo dei possibili indirizzi. L'indirizzo IP con cui è possibile raggiungere il Gigaset SE366 WLAN dall'esterno viene fornito dall'Operatore di rete.

➞ Se si desidera assegnare al Gigaset SE366 WLAN un indirizzo IP diverso, immettere tale indirizzo nei campi accanto a ***Indirizzo IP***.

➞ Se si desidera utilizzare una maschera di sottorete diversa, digitarla nel campo ***Subnet mask***. È possibile modificare solo l'ultimo campo.

Si consiglia di utilizzare un indirizzo dell'intervallo indirizzi riservato all'utilizzo privato. L'intervallo indirizzi è 192.168.1.1 – 192.168.255.254.

Avvertenza:

le nuove impostazioni vengono applicate solo dopo il riavvio del Gigaset SE366 WLAN. Se necessario, riconfigurare l'indirizzo IP del proprio PC (assegnarne anche uno nuovo) per riconciliarlo nella nuova configurazione.

Configurazione del server DHCP

Il Gigaset SE366 WLAN dispone di un Server DHCP che alla consegna è attivato. Gli indirizzi IP dei PC vengono assegnati, quindi, automaticamente dal Gigaset SE366 WLAN.

Avvertenza:

- se il server DHCP del Gigaset SE366 WLAN è attivato, è possibile configurare l'impostazione di rete dei PC in modo che sia impostata l'opzione ***Ottieni automaticamente un indirizzo IP***. A questo proposito leggere il documento „Das lokale Netzwerk konfigurieren“ sul CD.
- Quando si disattiva il server DHCP, è necessario assegnare un indirizzo IP statico ai PC tramite l'impostazione di rete.

➞ Per attivare il server DHCP selezionare ***Attivo***.

➞ Quando il server DHCP è attivo, è possibile stabilire il ***Tempo di lease***. La Scadenza stabilisce il tempo durante il quale il PC mantiene l'indirizzo IP assegnato senza modificarlo.

Avvertenza:

se si seleziona l'opzione ***Non scade mai*** gli indirizzi IP non vengono mai modificati. È necessario selezionare questa opzione se si desidera eseguire le impostazioni NAT o firewall con cui utilizzare gli indirizzi IP dei PC oppure occorre assegnare a questi PC indirizzi IP statici.

➞ Immettere l'intervallo degli indirizzi IP che il Gigaset SE366 WLAN deve utilizzare per assegnare automaticamente gli indirizzi IP ai PC. Immettere l'***Indirizzo IP emesso per primo*** e l'***Indirizzo IP emesso per ultimo***.

➞ Nel campo ***Nome del dominio*** è possibile fornire il nome di un dominio (gruppo di lavoro Windows).

Assegnazione di indirizzi IP statici a singoli PC

Quando è stato attivato un server DHCP, è ugualmente possibile assegnare un indirizzo IP statico a singoli PC (ad es. se impostano questi PC per le funzioni NAT).

➞ Immettere l'***Indirizzo MAC*** e il nome del PC nel campo ***Nome dispositivo***.

➞ Immettere l'***Indirizzo IP*** che si desidera assegnare al PC nel campo sottostante.

➞ Fare clic su ***Aggiungi*** per aggiungere la voce all'elenco.

➞ Fare clic sul pulsante ***Cancella*** per cancellare la voce all'elenco.

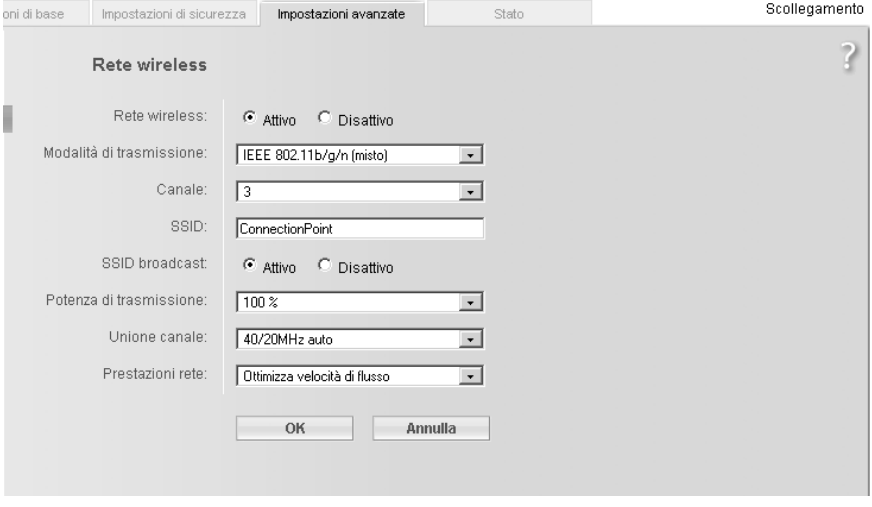
➞ Fare clic su ***OK*** per confermare le impostazioni.

Configurazione per connessioni wireless

Se i PC comunicano tra loro wireless attraverso il Gigaset SE366 WLAN, è necessario adottare misure per aumentare la protezione della rete wireless. La configurazione si effettua nel menu ***Impostazioni avanzate*** – ***Rete wireless***. È possibile

- attivare il modulo wireless Gigaset SE366 WLAN (vedere oltre),
- impostare canale e SSID (v. pag. 66),
- Attivare e configurare WPS (v. pag. 68),
- impostare la Crittografia del traffico (v. pag. 69),
- limitare l'accesso alla rete locale del Gigaset SE366 WLAN (v. pag. 74),
- configurare la funzione di ripetitore del Gigaset SE366 WLAN (v. pag. 75).

➞ Nel menu ***Impostazioni avanzate*** selezionare la voce ***Rete wireless***.



➥ Selezionare l'opzione ***Attivo*** per ***Rete wireless*** (predefinita).

Solo quando è attivato il modulo wireless del Gigaset SE366 WLAN è possibile collegare gli apparecchi wireless.

Ora è possibile eseguire le impostazioni per la rete wireless.

Modalità di trasmissione

La Modalità di trasmissione stabilisce lo standard IEEE sulla base del quale i dati vengono scambiati nella rete. IEEE 802.11g permette una velocità di trasmissione dati massima di 54 Mbps, IEEE 802.11b fino a 11 Mbps. IEEE 802.11n (Draft, v. pag. 15) raggiunge invece una velocità di trasmissione dei dati massima di 300 Mbps.

➥ Per le migliori velocità di trasmissione dati possibili nella propria rete scegliere ***IEEE 802.11b/g/n (misto)***.

SSID

Per consentire la comunicazione tra i componenti di rete in collegamento wireless, è necessario utilizzare lo stesso SSID (Service Set Identifier).

Avvertenza:

Se si è già effettuata una registrazione WPS (v. pag. 68), su questa pagina si vede l'SSID generato. L'SSID generato da WPS non andrebbe cambiato a mano in nessun caso. In caso contrario i client registrati non hanno più accesso alla rete wireless.

Al momento della consegna il Gigaset SE366 WLAN è dotato di SSID **ConnectionPoint**. Se non si usa WPS, l'SSID andrebbe cambiato.

Per motivi di sicurezza, disattivare l'SSID-Broadcast (v. pag. 67).

Per modificare a mano l'SSID, digitare una stringa di caratteri a scelta. Viene fatta distinzione tra caratteri maiuscoli e minuscoli. Essa può essere composta da 32caratteri alfanumerici.

Avvertenza:

la connessione agli adattatori di rete wireless viene interrotta fino a quando non viene immesso il nuovo SSID.

Canale

Il canale radio impostato viene utilizzato da tutti i client della rete per la trasmissione di dati wireless. A seconda della località, sono disponibili diversi canali.

➥ Selezionare il canale per la trasmissione dati.

SSID broadcast

Se l'opzione è attivata (predefinita), il Gigaset SE366 WLAN invia l'SSID con tutte le trasmissioni di dati e l'SSID del Gigaset SE366 WLAN viene visualizzato sui PC dotati di adattatore di rete wireless. In questo caso è possibile che persone non autorizzate, in ascolto sulla rete, tramite l'SSID riescano ad accedervi.

Quando viene disattivata l'opzione ***SSID broadcast*** l'SSID del Gigaset SE366 WLAN non viene visualizzato. In tal modo viene aumentata la protezione da attacchi non autorizzati della rete wireless. Annotarsi comunque l'SSID Esso è necessario per il login del proprio PC.

➡ Selezionare l'opzione ***Disattivo*** per disattivare ***SSID broadcast***.

Potenza di trasmissione

➡ Scegliere la prestazione di invio desiderata del proprio apparecchio.

Si consiglia di scegliere la potenza dei trasmissione in modo che la portata sia adatta alla situazione ambientale della rete locale. Una portata molto superiore consente facilmente l'ascolto non autorizzato della trasmissione dati wireless.

Unione canale

È possibile utilizzare la ***Unione canale*** solo se questa funzione viene supportata da almeno un client della rete wireless. Per ottenere la migliore velocità di trasmissione dati è necessario che tutti i client della rete locale supportino la funzione di ***Unione canale***.

➡ Selezionare un valore per l'***Unione canale*** dall'elenco: ***20 MHz***, ***40 MHz*** o ***40/20 MHz Auto*** (impostazione predefinita).

Prestazioni rete

Le Prestazioni rete possono essere ottimizzate nel modo seguente:

- ***Ottimizza velocità di flusso***
  rende massima la velocità di trasmissione dati nella rete ed assicura una trasmissione immediata del traffico di dati.
- ***Ottimitta risparmio energetico***
  ottimizza il consumo di corrente per prolungare l'intervallo di standby di apparecchi mobili nella rete come ad esempio notebook, PDA e headset WLAN.
- ***Personalizzato***
  In tal modo è possibile adattare le Prestazioni rete alle proprie necessità anche con l'aiuto delle seguenti grandezze:
  - ***Intervallo beacon*** stabilisce l'intervallo tra due Beacons.
    L'unità è millisecondi, valore predefinito 100 msecs.
  - ***Intervallo DTIM*** stabilisce l'intervallo tra due richiami (DTIM) per gli apparecchi che si trovano nella modalità di risparmio energetico.
    L'unità è il numero di beacon, il valore predefinito è 2 beacon.

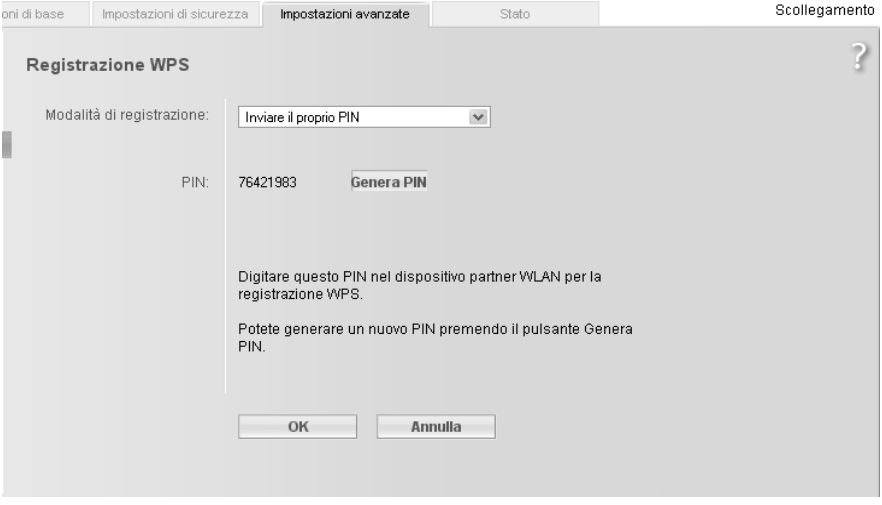
➡ Scegliere le ***Prestazioni rete*** desiderate.

Impostare WPS

Wi-Fi Protected Setup (WPS) facilita la realizzazione di una rete wireless. Gli apparecchi dotati di WPS possono generare automaticamente un SSID e una chiave WPA (Pre-Shared Key, vedi sopra) e sincronizzarsi tra loro.

Premendo il tasto di registrazione e con un solo clic (1 click only) nell'interfaccia di configurazione del client, è possibile stabilire una connessione wireless sicura. Ulteriori informazioni sull'installazione si trovano nel capitolo “WPS“ a pagina 13.

➥ Nel menu ***Rete wireless*** selezionare la voce ***Registrazione WPS***.



➥ Selezionare la ***Modalità di registrazione*** desiderata:

– ***Premere il pulsante***

Cliccare su ***OK*** per avviare la registrazione WPS.

Questa funzione corrisponde alla pressione del tasto di registrazione sul retro dell'apparecchio.

Dopo l'avvio della registrazione WPS viene cercato un client WPS all'interno del raggio di azione. Un client WPS il raggio di azione WLAN che attiva la propria funzione WPS entro 2 minuti, ottiene i dati di sicurezza del Gigaset SE366 WLAN (SSID e Pre-shared Key) è dentro il modo registrato.

La procedura di registrazione viene visualizzata nella finestra.

La procedura di registrazione può essere seguita sulla base del LED (v. pag. 19).

– ***Inviare il proprio PIN***

Viene visualizzato il PIN generato automaticamente.

Se si desidera generare un nuovo PIN, cliccare su ***Genera PIN***. Notare che gli eventuali apparecchi collegati alla rete con il PIN vecchio, non avranno più accesso al Gigaset SE366 WLAN.

Cliccare su ***OK*** per attivare le impostazioni.

Digitare il PIN generato in tutti gli apparecchi partner WLAN che devono stabilire una connessione.

– ***Digitare il PIN del dispositivo partner***

L'opzione si usa solo nel caso in cui nella WLAN si usa un PIN di un altro apparecchio. Digitare il PIN dell'apparecchio partner WLAN e cliccare su ***OK*** per attivare l'impostazione. Tale PIN deve essere usato in tutti gli apparecchi partner WLAN per la registrazione al Gigaset SE366 WLAN.

Avvertenza:

Se si è attivato il controllo di accesso tramite i filtri MAC, notare che la registrazione tramite WPS sarà possibile solo a quei client registrati nella lista degli indirizzi MAC.

Impostare la crittografia

Per proteggere la rete locale wireless dall'ascolto non autorizzato dall'esterno o dall'accesso non autorizzato ai dati è necessario impostare la crittografia dei dati.

Avvertenza:

Se sì è già effettuata una registrazione WPS, è allora impostata la crittografia WPA2-PSK/WPA-PSK. La seguente descrizione vale solo se non si utilizza WPS.

➡ Scegliere nel menu ***Rete wireless*** la voce ***Crittografia***.

È possibile utilizzare i seguenti meccanismi di protezione:

- WPA2-PSK e WPA2-PSK / WPA-PSK (v. pag. 69)
- WPA2 e WPA2 / WPA con server di autenticazione (v. pag. 70)
- Crittografia WEP (Wired Equivalent Privacy), (v. pag. 71).

WPA2-PSK e WPA2-PSK / WPA-PSK

Avvertenza:

Se si è già effettuata una registrazione WPS, (vedi pagina 13 o pagina 68), su questa pagina si vede la Pre-shared Key generata. Se non si desidera usare WPS, qui si può cambiare la crittografia. In tal caso si dovranno configurare a mano tutti gli adattatori di rete wireless.

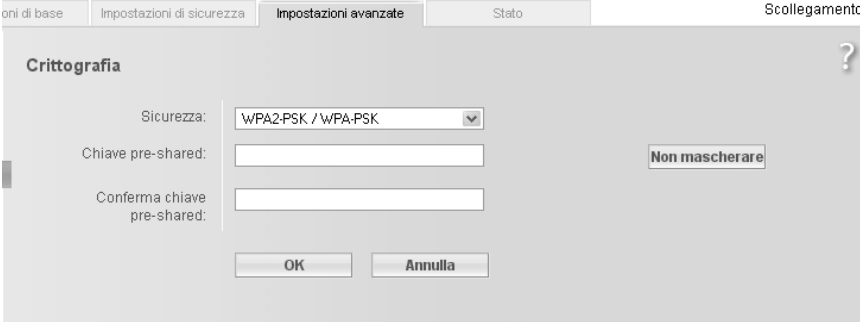
Se si è prima eseguita la crittografia a mano e se poi si effettua una registrazione WPS, le impostazioni manuali della crittografia verranno sovrascritte. Si dovranno poi registrare tutti gli adattatori di rete wireless tramite WPS così dovrà digitare nuovamente a mano la crittografia generata tramite WPS negli adattatori di rete..

WPA con Pre-shared Key (WPA-PSK)

WPA-PSK è una modalità WPA speciale per l'utente privato e le piccole aziende senza server di autenticazione che fornisce una protezione forte mediante crittografia. La chiave di crittografia viene creata automaticamente con la Pre-shared Key e modificata automaticamente ("Rekeying") e dopo un lasso di tempo prestabilito viene autenticata tra gli apparecchi (Intervallo di rekey).

Lo standard della crittografia da selezionare dipende dai componenti della rete wireless. Ciascun PC (adattatore di rete) che accede a una rete wireless, protetta con WPA, deve a sua volta supportare il WPA. Per le modalità di utilizzo del WPA sul proprio PC, consultare le istruzioni d'uso dei propri adattatori di rete. Se tutti i componenti supportano lo standard WPA2, selezionare l'opzione ***WPA2-PSK***. Se si utilizza l'adattatore di rete che supporta solo WPA, selezionare l'opzione ***WPA2-PSK / WPA-PSK***. Gli inserimenti di seguito descritti sono uguali per entrambe le opzioni.

➞ Nel campo ***Sicurezza*** selezionare l'opzione desiderata.



➞ Nel campo ***Chiave pre-shared*** immettere una chiave (fino a 63 caratteri alfanumerici) e confermarla con ulteriore immissione.

➞ Se si clicca su ***Non mascherare***, viene visualizzata una finestra informativa della Pre-shared Key a caratteri leggibili.

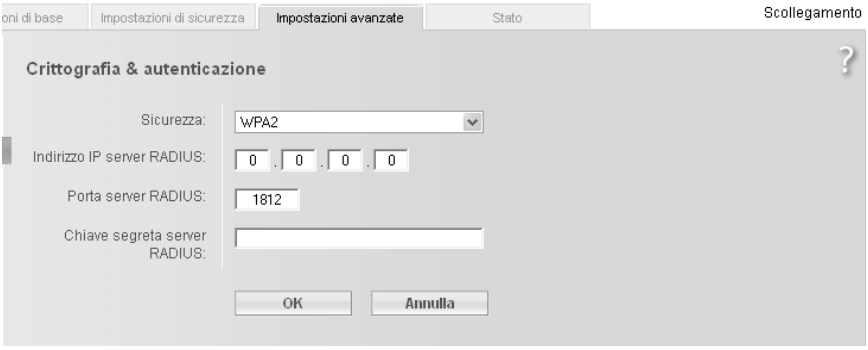
➞ Per copiare le impostazioni, fare clic su ***OK***.

WPA e WPA2 con server di autenticazione

Nelle reti grandi (ad es. nelle aziende) lo standard WPA consente l'utilizzo di un servizio aggiuntivo di autenticazione. In questo caso l'accesso utente alla crittografia WPA viene controllato con account utente e password. Un server RADIUS funge da server di autenticazione. È possibile selezionare il nuovo standard ***WPA2*** se viene supportato da tutti i componenti della rete wireless oppure selezionare ***WPA2 / WPA*** se si utilizzano apparecchi che supportano soltanto il WPA.

Se si utilizza WPA2/WPA, l'utilizzo WPS non è possibile.

➞ Nel campo ***Sicurezza*** selezionare l'opzione desiderata.



➞ Nel campo ***Indirizzo IP server RADIUS*** immettere l'indirizzo IP del server RADIUS.

➞ Nel campo ***Porta server RADIUS*** immettere la porta del server RADIUS.

➞ Nel campo ***Chiave segreta server RADIUS*** immettere una parola chiave corrispondente alle convenzioni del server RADIUS che deve essere utilizzata dal server per l'autenticazione.

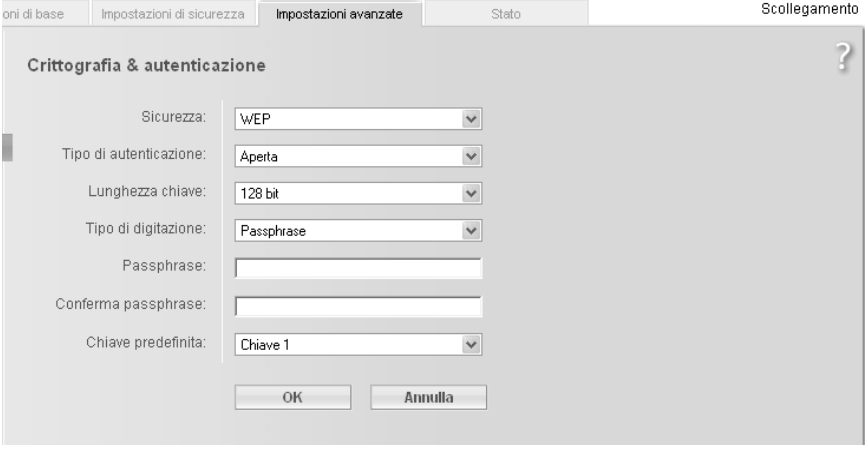
➞ Fare clic su ***OK*** per confermare le impostazioni.

Crittografia WEP

Qualora WPA non sia supportato da tutti i componenti della rete wireless, si consiglia di attivare nei componenti della rete wireless la WEP-Crittografia.

Avvertenza:
Con la crittografia WEP l'utilizzo della funzione WPS non è possibile.

➞ Nel campo ***Sicurezza*** selezionare l'opzione ***WEP***.



➥ Selezionare un ***Tipo di autenticazione***:

- Selezionare ***Condivisa*** per ottenere da ciascun client la registrazione alla rete con chiave stabilita.
- Selezionare ***Aperta*** per consentire la trasmissione dati nella rete wireless anche senza immissione di una chiave.

Per applicare la crittografia è possibile scegliere tra la chiave standard a 64-Bit oppure la chiave più potente a 128-Bit. La chiave viene generata in formato esadecimale oppure in formato ASCII. È necessario utilizzare la stessa chiave per la crittografia e la decrittazione sia per il Gigaset SE366 WLAN sia per tutti gli adattatori di rete wireless.

➥ Selezionare la ***Lunghezza chiave***: 64 oppure 128-Bit.

➥ Selezionare il ***Tipo di digitazione***, cioè se la chiave deve essere inserita manualmente o deve essere generata automaticamente attraverso una ***Passphrase***.

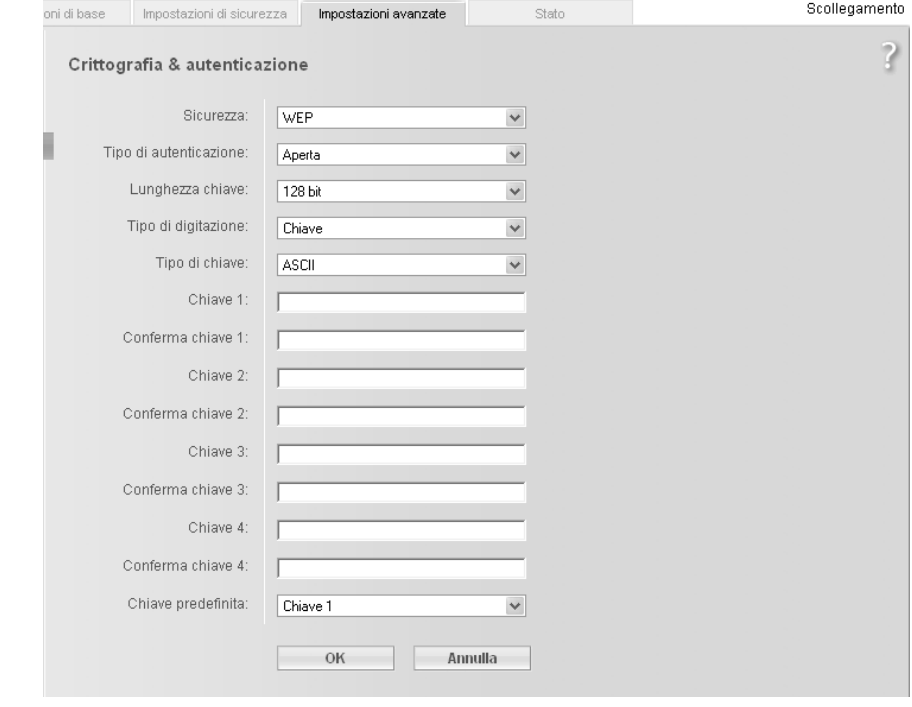
Generazione della chiave tramite Passphrase

➥ Immettere una ***Passphrase*** (fino a 32 caratteri) e confermare con ulteriore immissione. Vengono generate quattro chiavi.

➥ Selezionare una delle quattro chiavi come ***Chiave predefinita***.

Inserimento manuale della chiave

➥ Selezionare il ***Tipo di chiave***, ***Hex*** oppure ***ASCII***.



Se si sceglie ***Hex***, è possibile utilizzare i numeri da **0** fino a **9** e le lettere da **A** fino a **F**.

– Con una chiave a 64 Bit, la lunghezza è di 10 caratteri.
  Esempio di chiave valida: 1234567ABC
– Con una chiave a 128 Bit, la lunghezza è di 26 caratteri.
  Esempio di chiave valida: 234567ABC8912345DEF1234567

Se si sceglie***ASCII***, è possibile utilizzare i numeri da **0** fino a **9**, i caratteri da **A** fino a **Z** e da **a** fino a **z** e i caratteri speciali ASCII.

– Con una chiave a 64 Bit, la lunghezza è di 5 caratteri.
  Esempio di chiave valida: GIGA1
– Con una chiave a 128 Bit, la lunghezza è di 13 caratteri.
  Esempio di chiave valida: GIGASET_SE336

➔ Immettere fino a quattro chiavi nei campi ***Chiave 1*** fino a ***Chiave 4*** e confermarle con ulteriore immissione nei campi
Conferma chiave 1 fino a***Conferma chiave 4***.

➔ Selezionare una delle quattro chiavi come ***Chiave predefinita***.

Avvertenza:

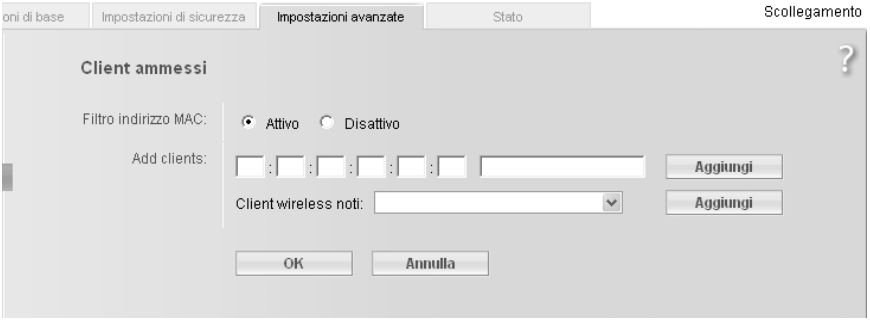
- è molto **importante** annotare la chiave ovvero la stringa. Queste informazioni sono importanti per configurare in modo corretto l'adattatore di rete wireless;
- dopo aver terminato la configurazione, è necessario anche modificare la crittografia WEP negli adattatori dei PC poiché, in caso contrario, non sarà più possibile accedere alla rete wireless del Gigaset SE366 WLAN.

➔ Cliccare su ***OK*** per confermare le impostazioni.

Client ammessi

In questa pagina è possibile stabilire quali PC possono avere accesso wireless al Gigaset SE366 WLAN e, quindi, alla propria rete locale.

➞ Scegliere nel menu ***Rete wireless*** la voce ***Client ammessi***.



Nei parametri iniziali il controllo di accesso è disattivato. Ciò significa che possono collegarsi tutti i PC che utilizzano il SSID corretto.

Il controllo di accesso si basa sull'Indirizzo MACdegli adattatori di rete dei PC.

➞ Attivare il controllo di accesso con l'opzione ***Attivo*** del campo ***Filtro indirizzo MAC***.

Immissione manuale dei PC:

➞ Immettere i PC desiderati con ***Indirizzo MAC*** e ***Nome dispositivo*** nei campi corrispondenti;

➞ Fare clic su ***Aggiungi*** per aggiungere la voce all'elenco.

➞ Fare clic sul pulsante ***Cancella*** per cancellare la voce all'elenco.

➞ Fare clic su ***OK*** per confermare le impostazioni.

Scelta dall'elenco dei PC collegati

➞ Selezionare dall'elenco ***Client wireless noti*** (tutti i PC che hanno accesso diretto al Gigaset SE366 WLAN) il PC che si desidera aggiungere al controllo di accesso.

➞ Fare clic su ***Aggiungi*** per aggiungere la voce all'elenco.

➞ Fare clic su ***OK*** per confermare le impostazioni.

Avvertenze:

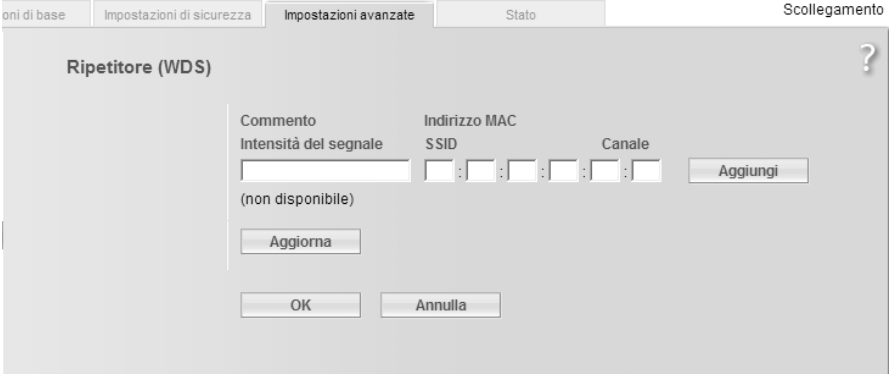
- Se si è attivato il controllo di accesso tramite i filtri MAC e si intende utilizzare WPS, notare che la registrazione sarà possibile solo a quei client registrati nella lista degli indirizzi MAC.
- quando si attiva il controllo di accesso MAC, è necessario immettere almeno il PC dal quale si configura il Gigaset SE366 WLAN. In caso contrario non sarà più possibile accedere all'interfaccia operativa e viene visualizzato il relativo messaggio di errore.
- Qualora per errore fosse stato negato a tutti i PC l'accesso al Gigaset SE366 WLAN sono disponibili due opzioni:
  - È possibile reimpostare completamente il Gigaset SE366 WLAN sulle impostazioni di fabbrica (v. pag. 20).
  - È possibile collegare un PC con connessione LAN al Gigaset SE366 WLAN. Poiché il controllo di accesso MAC è valido solo per i PC collegati wireless, è possibile modificare la configurazione da questo PC.

Funzione Ripetitore (WDS)

Quando si utilizza un Repeater per aumentare la portata nella rete wireless, è necessario attivare la funzione Wireless Distribution System (WDS).

➡ Nel menu ***Impostazioni avanzate*** – ***Rete wireless*** selezionare la voce ***Ripetitore (WDS)***.

Vengono cercati tutti gli Access Point e ripetitori disponibili nel un raggio di azione e visualizzati con il relativo SSID, indirizzo MAC, canale e intensità di segnale.



➡ Fare clic su ***Aggiorna*** per aggiornare la visualizzazione.

➡ Cliccare su ***Aggiungi*** per scegliere un apparecchio come ripetitore della rete wireless.

➡ Fare clic su ***Cancella*** per cancellare un apparecchio come ripetitore.

➡ Fare clic su ***OK*** per confermare le impostazioni.

Le impostazione di crittografia nel ripetitore devono essere corrispondenti a quelle del-Gigaset SE366 WLAN. Se il ripetitore supporta WPS, è possibile effettuare la registrazione tramite WPS. Informazioni più dettagliate possono essere trovate nelle istruzioni d'uso del ripetitore.

Se si utilizza WPS o la crittografia WPA2-PSK/WPA-PSK, è possibile utilizzare un ripetitore, con la crittografia WEP un massimo di 6 ripetitori attraverso la funzione WDS nella propria rete wireless.

Amministrazione e informazioni sullo stato

L'interfaccia utente del Gigaset SE366 WLAN contiene funzioni utili per la gestione. È possibile

- stabilire una connessione manuale a Internet (vedere oltre),
- eseguire impostazioni internazionali (v. pag. 78),
- modificare la password del sistema (v. pag. 79),
- impostare la gestione remota (v. pag. 80),
- salvare i dati di configurazione e se necessario ripristinarli (v. pag. 82),
- reimpostare il Gigaset SE366 WLAN sulle impostazioni iniziali (v. pag. 83),
- riavviare l'apparecchio (v. pag. 83),
- aggiornare il firmware (v. pag. 84),
- eseguire impostazioni per il registro eventi di sistema (v. pag. 85),
- attivare o disattivare il tasto di registrazione (v. pag. 86)
- informarsi sulla configurazione e lo stato del Gigaset SE366 WLAN (v. pag. 87).

Istituzione manuale di connessioni Internet

È possibile stabilire una connessione manuale a Internet.

Per avviare o concludere manualmente una connessione a Internet:

➡ Aprire la pagina iniziale del Gigaset SE366 WLAN come descritto a pagina 26.

Se è già stata avviata l'interfaccia di configurazione, fare clic sulla scheda ***Home*** in alto a sinistra della finestra.

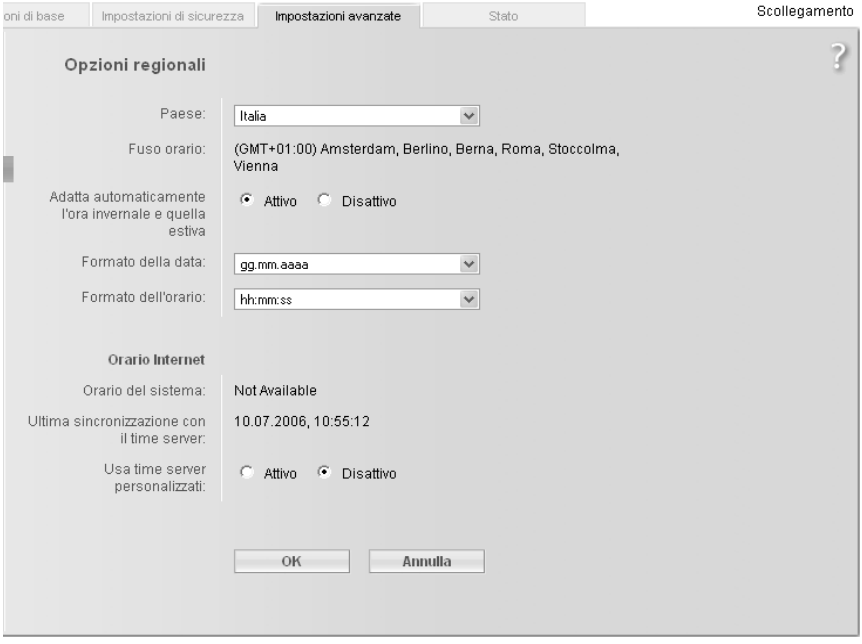
Se l'interfaccia di configurazione non è ancora stata avviata, avviarla ora ed effettuare il login.

➡ Fare clic su ***Connetti*** per stabilire una connessione Internet.

Opzioni regionali

È possibile scegliere per il proprio Gigaset SE366 WLAN il luogo, il fuso orario e il formato per data e ora oltre a configurare l'utilizzo di un server di riferimento per l'ora Internet.

➥ Nel menu ***Impostazioni avanzate*** – ***Amministrazione*** selezionare la voce ***Opzioni regionali***.



➥ Selezionare dall'elenco il Paese corrispondente. A seconda della scelta, è possibile eseguire le impostazioni per la conversione automatica dell'ora legale e/o del ***Fuso orario***.

➥ Selezionare l'opzione desiderata e/o scegliere il ***Fuso orario*** della propria località.

➥ Scegliere dagli elenchi***Formato della data*** e ***Formato dell'orario*** il formato desiderato per l'inserimento di data e ora.

Orario Internet

Il ***Orario del sistema*** dell'apparecchio viene sincronizzato automaticamente con il server di riferimento in Internet. Per informazione dell'utente, viene visualizzato il momento dell'***Ultima sincronizzazione con il time server***.

➥ Se si desidera utilizzare un proprio server di riferimento, selezionare l'opzione ***Attivo*** accanto al campo ***Usa time server personalizzati***.

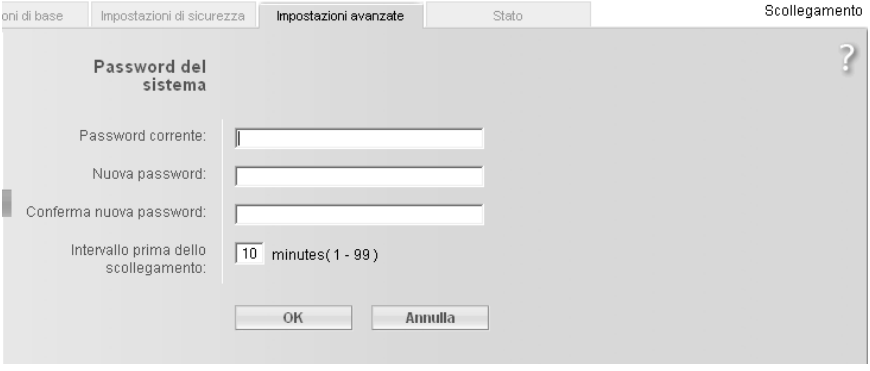
➥ Inserire nei campi ***Time server preferito*** e ***Time server alternativo*** l'indirizzo Internet del server di riferimento.

➥ Fare clic su ***OK*** per confermare le impostazioni.

Password del sistema

È possibile digitare e stabilire la Password del sistema per l'interfaccia di configurazione del Gigaset SE366 WLAN, ed è possibile stabilire dopo quale intervallo viene automaticamente terminata una sessione se non avviene alcuna immissione.

➥ Scegliere nel menu ***Amministrazione*** la voce ***Password del sistema***.



Dopo l'installazione la configurazione del Gigaset SE366 WLAN di norma è protetta con la Password del sistema ***admin***. Per evitare che persone non autorizzate possano eseguire modifiche alla configurazione, si consiglia di inserire una propria Password del sistema e di modificarla periodicamente.

➥ Se è stata già immessa una Password del sistema, inserire la vecchia Password del sistema nel campo ***Password corrente***.

➥ Immettere una nuova password nel campo ***Nuova password*** e ripeterla nel campo ***Conferma nuova password***.

La password può comprendere al massimo 32 caratteri. Viene fatta distinzione tra caratteri maiuscoli e minuscoli. Non utilizzare nomi propri o concetti facilmente indovinabili. Utilizzare combinazioni di lettere, numeri e caratteri speciali.

Avvertenza:

qualora si sia dimenticata la propria Password del sistema, è necessario reimpostare il Gigaset SE366 WLAN (v. pag. 21). Tenere conto che in tal modo sono state reimpostate **tutte** le immissioni sulle impostazioni iniziali. Come standard al momento della consegna è preimpostata la password ***admin***.

Impostazione dell'Intervallo prima dello scollegamento

➡ Inserire l'intervallo in minuti dopo il quale il programma di configurazione viene interrotto se non avviene alcuna immissione. Il valore predefinito è 10 minuti.

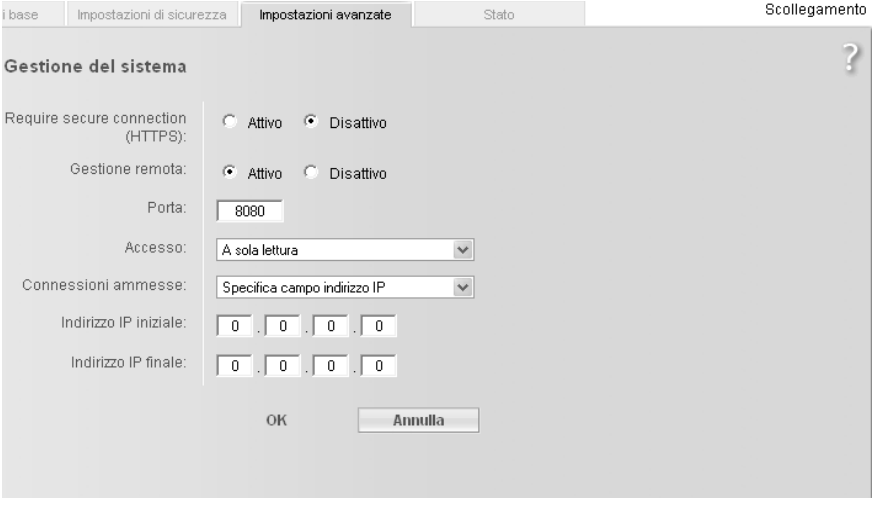
➡ Fare clic su ***OK*** per confermare le impostazioni.

Impostazione della Gestione remota

Con la Gestione remota il PC che non è nella rete locale può configurare il Gigaset SE366 WLAN con l'aiuto di un browser da remoto. È possibile consentire la Gestione remota per un determinato PC o per qualsiasi PC.

Per la propria protezione, questa funzione è disponibile se la password di sistema dell'apparecchio è stata modificata in precedenza (v. pag. 79).

➡ Scegliere nel menu ***Amministrazione*** la voce ***Gestione del sistema***.



➡ ***Richiede connessione sicura (HTTPS)***

Attivare questa funzione se si intende scegliere il protocollo sicuro HTTPS attraverso il quale un PC può accedere dall'esterno al Gigaset SE366 WLAN.

In caso contrario viene utilizzato il protocollo HTTP.

➡ Per la ***Gestione remota*** selezionare l'opzione ***Attivo***, se si desidera consentire la Gestione remota.

È possibile avviare la gestione remota immettendo l'indirizzo IP pubblico nel proprio browser. Poiché esso spesso viene assegnato nuovamente dall'operatore di rete a ogni nuovo collegamento, si consiglia di utilizzare il DNS dinamico (v. pag. 61).

➞ È possibile modificare la ***Porta*** con cui si accede al programma di configurazione da Internet, per es. per nascondere il programma di configurazione ad accessi non autorizzati.

➞ Stabilire nel campo ***Accesso*** per le connessioni autorizzate quale diritto di accesso ***Accesso (illimitato)*** o ***Accesso (sola lettura)***.

➞ ***Connessioni ammesse:*** è possibile stabilire un determinato PC o tutti i PC di un determinato campo di indirizzi IP per la Gestione remota o permettere questa funzione a qualsiasi PC. Selezionare l'opzione desiderata dall'elenco.

Avvertenza:
se si consente l'accesso a qualsiasi PC, chiunque trovi la password ha accesso all'interfaccia operativa e quindi alla rete! Si consiglia di attivare questa opzione, se necessario, soltanto per breve tempo.

Gestione remota per un determinato PC:

➞ immettere nel campo ***Indirizzo IP*** l'indirizzo IP del PC che deve avere accesso all'interfaccia operativa dall'esterno della rete locale del Gigaset SE366 WLAN.

Gestione remota per un PC di un determinato campo d'indirizzi IP:

➞ Definire nei campi ***Indirizzo IP iniziale*** e ***Indirizzo IP finale*** il campo di indirizzi IP del PC che deve avere accesso dall'esterno all'interfaccia operativa del Gigaset SE366 WLAN.

Avvertenza:
- l'operatore di rete assegna al PC eventualmente l'indirizzo IP in modo dinamico. Quindi può cambiare. Assicurarsi che il PC, dal quale si accede al router di Internet, abbia sempre lo stesso indirizzo IP.
- Per accessi all'interfaccia di configurazione tramite Gestione remota è necessario immettere nel browser l'indirizzo del Gigaset SE366 WLAN nel formato seguente: **`http://X.X.X.X:8080`** (x.x.x.x sta per indirizzo IP del Gigaset SE366 WLAN).

➞ Fare clic su ***OK*** per confermare le impostazioni.

Salvataggio e ripristino della configurazione

Dopo aver configurato il Gigaset SE366 WLAN, è utile salvare questa configurazione. Nel caso in cui le impostazioni dovessero essere cancellate o sovrascritte per sbaglio, è infatti possibile recuperare quanto salvato.

Inoltre è possibile reimpostare la configurazione alle impostazioni iniziali. Si consigliare di farlo in ogni caso prima di consegnare l'apparecchio a terzi.

◆ Scegliere nel menu ***Amministrazione*** la voce ***Salva & ripristina***.

Salvataggio dei dati di configurazione

➥ Selezionare l'opzione ***Salva configurazione***.

Si apre una finestra di dialogo in cui è possibile immettere i dati dove devono essere memorizzati i file di backup.

➥ Selezionare quindi una cartella sul proprio PC locale, nella quale salvare il file di configurazione e inserire un nome per il file.

➥ Fare clic sul pulsante ***Salva***.

Al termine della procedura i dati di configurazione correnti vengono salvati nel file indicato.

Ripristino del backup

➥ Contrassegnare l'opzione ***Ripristina configurazione***.

➥ Scegliere nel file system il file con il quale si desidera ripristinare la configurazione.

➥ Confermare la procedura della finestra di dialogo che segue cliccando su ***OK***.

➥ Cliccare su ***OK***. La configurazione viene ora aggiornata.

Ripristino delle impostazioni iniziali

È possibile riportare il Gigaset SE366 WLAN alle impostazioni iniziali. Questa procedura deve essere eseguita prima di consegnare l'apparecchio ad altre persone oppure prima di una sostituzione presso il rivenditore. In caso contrario persone non autorizzate potrebbero utilizzare i propri dati di accesso a Internet con il conseguente addebito dei relativi costi.

➥ Selezionare l'opzione ***Reimpostare la configurazione sui valori di fabbrica*** e fare clic su ***OK***.

➥ Confermare la procedura della finestra di dialogo che segue cliccando su ***OK***.

Avvertenza:

è possibile riavviare il Gigaset SE366 WLAN se non funziona più correttamente. Alla fine esso dovrebbe essere di nuovo pronto all'uso (v. pag. 20).

Tenere conto che in caso di reset completo **tutte** le impostazioni di configurazione vengono reimpostate alle impostazioni iniziali. Ciò significa che il Gigaset SE366 WLAN dovrà essere del tutto riconfigurato.

Reboot

È possibile riavviare il Gigaset SE366 WLAN se non funziona più correttamente. È poi di nuovo pronto all'uso.

➥ Scegliere nel menu ***Amministrazione*** la voce ***Reboot***.

➥ Fare clic su ***OK*** per riavviare l'apparecchio.

Aggiornamento firmware

Qualora Gigaset o il proprio Operatore di rete forniscano una nuova versione di firmware, è possibile aggiornare il Gigaset SE366 WLAN. A questo scopo, è necessario scaricare il nuovo firmware sul proprio PC.

Procedere come descritto di seguito:

➞ Terminare tutte le attività di rete nella propria rete locale.

➞ Scegliere nel menu ***Amministrazione*** la voce ***Aggiornamento del firmware***.

Nella colonna ***Versione corrente del firmware*** viene visualizzata la versione del firmware attualmente in uso sull'apparecchio.

➞ Nel campo ***File di aggiornamento del firmware*** immettere il file del nuovo firmware scaricato da Internet.

➞ Cliccare su ***OK***.

Il firmware viene ora aggiornato.

Avvertenza:

Non disattivare il Gigaset SE366 WLAN durante la procedura di aggiornamento. Questa procedura può richiedere alcuni minuti.

Dopo l'aggiornamento corretto, l'apparecchio viene riavviato automaticamente. Ciò richiederà un certo tempo. Dopo l'aggiornamento corretto viene nuovamente visualizzata la pagina di registrazione.

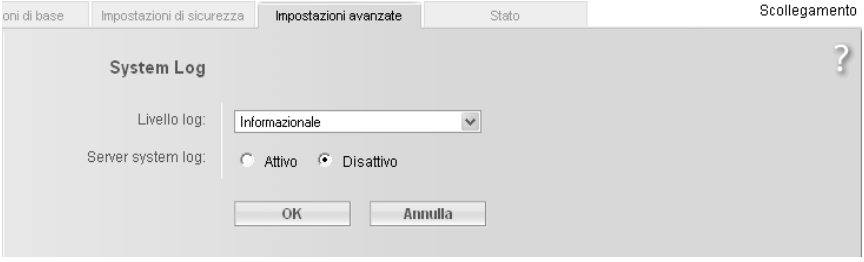
Avvertenza:

è possibile verificare nel menu ***Stato*** della pagina iniziale se la procedura di aggiornamento è stata eseguita correttamente (v. pag. 87). Qui viene visualizzata la versione attuale del firmware del Gigaset SE366 WLAN.

System Log

Il System Log viene visualizzato nel menu ***Stato*** – ***Dispositivo***. Possono essere riportate informazioni sulla funzione dell'apparecchio e sui possibili problemi. È possibile fornire queste informazioni in automatico a un server di registro eventi di sistema.

➡ Scegliere nel menu ***Amministrazione*** la voce ***System Log***.



➡ Effettuare per il protocollo le seguenti impostazioni:

- ***Livello log***: scegliere quante informazioni devono essere contenute nel registro eventi di sistema. Sono possibili quattro livelli:
  - ***Critico***: registrare le informazioni importanti per i possibili problemi nel funzionamento dell'apparecchio
  - ***Debug***: informazioni complete e dettagliate per tutte le funzioni dell'apparecchio
  - ***Attenzione*** e ***Informazionale*** rappresentano livelli intermedi.
- ***Server system log***
  - Attivare questa funzione se si desidera l'invio automatico del registro eventi di sistema dell'apparecchio a un server di registro nella rete locale.
  - ***Indirizzo server***:
    Immettere l'indirizzo IP del server degli eventi di sistema.
  - ***Porta server***:
    Immettere la porta del server di registro degli eventi di sistema che deve essere utilizzato per l'invio del registro eventi di sistema.

➡ Fare clic su ***OK*** per confermare le modifiche.

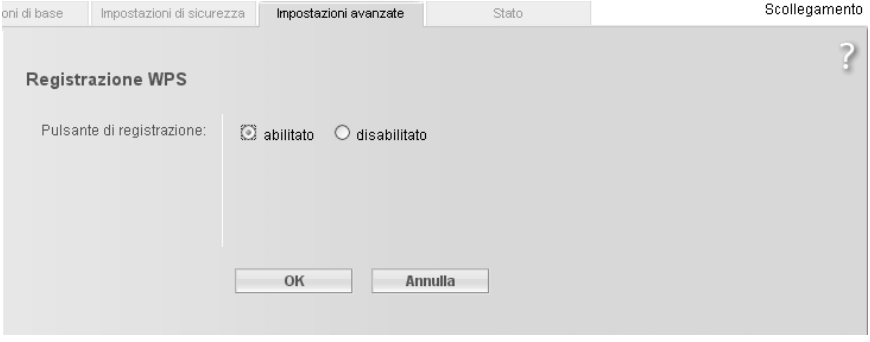
Disattivare il tasto di registrazione WPS

Il Gigaset SE366 WLAN supporta WPS per la configurazione automatica delle impostazioni di sicurezza nella rete wireless (v. pag. 13). La registrazione WPS può essere attivata tramite l'interfaccia operativa (v. pag. 68) o tramite il tasto di registrazione sul retro dell'apparecchio (v. pag. 20).

Dopo aver configurato la rete wireless, è possibile disattivare per motivi di sicurezza il tasto di registrazione in modo da impedire l'accesso al Gigaset SE366 WLAN a persone non autorizzate.

Come impostazione predefinita il tasto di registrazione è attivato.

➡ Scegliere nel menu ***Amministrazione*** la voce ***Pulsante di registrazione***.



➡ Selezionare l'opzione ***disabilitato***:

➡ Fare clic su ***OK*** per confermare le modifiche.

Informazioni sullo stato

Nel menu ***Stato*** del Gigaset SE366 WLAN è possibile informarsi sulla configurazione e sullo stato del Gigaset SE366 WLAN. Nella prima pagina è disponibile una panoramica sullo stato della connessione Internet, della rete locale e wireless e dell'apparecchio.

Per maggiori informazioni è possibile richiamare le seguenti pagine sullo stato:

- ***Sicurezza***
- ***Internet***
- ***Rete locale***
- ***Rete wireless***
- ***Dispositivo***

Per visualizzare la pagina sullo stato, procedere come segue:

→ Scegliere nella pagina iniziale la voce ***Stato***.

→ Scegliere la voce con le informazioni desiderate.

Panoramica

Nella prima pagina è disponibile una panoramica sullo stato operativo attuale e i dati più importanti dell'apparecchio.

Internet

- ***Stato della connessione***
  Lo stato della connessione a Internet e, se connesso, la durata della connessione.
- ***Indirizzo IP***
  L'indirizzo IP pubblico dell'apparecchio.

Rete locale

- ***Indirizzo IP***
  L'indirizzo IP locale dell'apparecchio.
- ***Server DHCP***
  Lo stato del server DHCP dell'apparecchio e, se attivato, il numero dei client della rete a cui è stato assegnato un indirizzo IP.

Rete wireless

- ***Stato***
  Lo stato della connessione di rete wireless dell'apparecchio e, se attivato, il numero dei client della rete wireless collegati all'apparecchio.
- ***SSID***
  L'identificazione della rete wireless.

Apparecchio

- ***Orario del sistema***
  L'ora del sistema dell'apparecchio.
- ***Versione del firmware***
  La versione del firmware installato sull'apparecchio.

➞ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Sicurezza

Alla pagina ***Sicurezza*** nel menu ***Stato*** sono disponibili informazioni sui possibili rischi di protezione per l'apparecchio e la rete.

- ***Password di sistema non cambiata***
  Il programma di configurazione dell'apparecchio non è protetto in modo efficace contro accessi non autorizzati poiché non è stata cambiata la password dalla messa in funzione. Nel capitolo "Password del sistema" a pagina 79 viene descritto come eliminare questo rischio di protezione.
- ***Identificazione della rete wireless visibile o non cambiata***
  La rete wireless è facile da trovare anche da parte di persone non autorizzate poiché l'identificazione della rete wireless (SSID) dalla messa in funzione non è stata modificata e la trasmissione del SSID (SSID-Broadcast) non è stata disattivata. Nel capitolo "Configurazione per connessioni wireless" a pagina 65 viene descritto come eliminare questo rischio di protezione.
- ***Crittografia per la rete wireless non attivata***
  Tutti i dati vengono trasmessi senza crittografia nella rete wireless e possono essere ascoltati con facilità. Inoltre, è possibile che utenti non autorizzati ottengano facile accesso alla rete, ai PC e alla connessione Internet. Nel capitolo "Impostare la crittografia" a pagina 69 viene descritto come eliminare questo rischio di protezione.
- ***Firewall per la connessione a Internet disattivato***
  La rete non è protetta contro accessi non autorizzati da parte di hacker da Internet. Nel capitolo "Firewall" a pagina 50 viene descritto come eliminare questo rischio di protezione.
- ***Traslazione indirizzi per la connessione a Internet disattivato***
  I client della rete non sono protetti contro accessi non autorizzati da Internet. Nel capitolo "Impostazione della funzione NAT" a pagina 56 viene descritto come eliminare questo rischio di protezione.

- ***Uno o più client locali esposti direttamente a Internet***

  Uno o più client della rete sono visibili come Exposed Host direttamente in Internet e, quindi, particolarmente esposti a rischi particolari (per es. ad attacchi di hacker). Questa funzione deve essere essere attivata soltanto se strettamente necessario (per es. per la gestione di un server web) e le altre funzioni non sono sufficienti (ad es. Port-Forwarding). In tal caso è necessario adottare misure adeguate ai singoli client. Nel capitolo "Apertura del firewall per determinati PC (Host esposto)" a pagina 60 viene descritto come eliminare questo rischio di protezione.

- ***Gestione remota attivata***

  Qualsiasi utente anche non autorizzato che conosca la password di sistema dell'apparecchio può accedere da Internet al programma di configurazione dell'apparecchio. Nel capitolo "Impostazione della Gestione remota" a pagina 80 viene descritto come eliminare questo rischio di protezione.

➡ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Internet

Alla pagina ***Internet*** nel menu ***Stato*** sono disponibili informazioni sullo stato della connessione Internet dell'apparecchio.

- ***Stato della connessione***

  Visualizza lo stato della connessione a Internet e, se connesso, la durata della connessione. Se come modalità di connessione è stata impostata ***Connessione su richiesta*** oppure ***Connessione manuale*** (v. pag. 45), è possibile ***Connetti*** o ***Disconnetti*** manualmente una connessione Internet.

- ***Modo di connessione***

  Visualizza lo modo di connessione impostato per la connessione a Internet.

- ***Indirizzo IP***

  Visualizza l'indirizzo IP pubblico del dispositivo.

- ***Indirizzo MAC***

  Visualizza l'indirizzo MAC pubblico dell'apparecchio.

- ***Gateway predefinito***

  Visualizza l'indirizzo IP del gateway predefinito utilizzato per la connessione a Internet corrente.

- ***Server DNS preferito***

  Visualizza l'indirizzo server DNS preferito utilizzato per la connessione a Internet corrente.

- ***Server DNS alternativo***

  Visualizza l'indirizzo server DNS alternativo utilizzato per la connessione a Internet corrente.

- ***Pass-through PPPoE***

  Visualizza lo stato del Pass-through PPPoE per il collegamento DSL via cavo per stabilire la connessione a Internet direttamente da un PC della rete.

- ***MTU***

  L'MTU definisce la lunghezza massima con la quale un pacchetto di dati può essere trasportato sulla rete senza frammentazione.

- ***Traslazione indirizzi (NAT)***
  - ***Stato***

    Visualizza lo stato della funzione NAT (Network Address Translation) per la connessione Internet.
  - ***Tabella NAT***

    Visualizza il numero delle voci attualmente disponibili nella tabella NAT.

    Fare clic su ***Vuoto*** per cancellare tutte le voci attualmente disponibili nella tabella NAT.
- ***DNS dinamico***
  - ***DNS dinamico***

    Visualizza lo stato del DNS dinamico per la connessione Internet.
  - ***Nome del dominio***

    Visualizza il nome del dominio per il DNS dinamico.

➥ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Rete locale

Alla pagina ***Rete locale*** nel menu ***Stato*** sono disponibili informazioni sulle impostazioni della rete locale.

- ***Indirizzo IP***

  Visualizza l'indirizzo IP locale dell'apparecchio.

- ***Subnet mask***

  Visualizza la maschera di sottorete utilizzata nella rete locale.

- ***Indirizzo MAC***

  Visualizza l'indirizzo MAC locale dell'apparecchio per la trasmissione dati via cavo.

- ***Server DHCP***
  - ***Stato***

    Visualizza lo stato del server DHCP dell'apparecchio per l'assegnazione automatica degli indirizzi IP ai client della rete locale.

- ***Client DHCP***

  Visualizza tutti i client della rete a cui è stato assegnato un indirizzo IP. Per l'identificazione vengono elencati per ciascun client il ***Nome host*** e l'***Indirizzo MAC***. Sono inoltre disponibili informazioni sull'***Indirizzo IP*** assegnato a ciascun client e sul ***Tempo di lease*** residuo dell'indirizzo IP prima che il client ne riceva uno nuovo dal server DHCP.

➞ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Rete wireless

Alla pagina ***Rete wireless*** nel menu ***Stato*** sono disponibili informazioni sulle impostazioni della rete wireless.

- ***Stato***

  Visualizza lo stato della connessione dell'apparecchio alla rete wireless.

- ***SSID***

  Visualizza l'identificazione della rete wireless.

- ***Canale***

  Visualizza il canale radio attualmente utilizzato per la trasmissione di dati nella rete locale.

- ***Indirizzo MAC***

  Visualizza l'indirizzo MAC locale dell'apparecchio per la trasmissione di dati wireless.

- ***Client wireless***

  Visualizza tutti i client della rete wireless al momento collegati all'apparecchio. Per l'identificazione vengono elencati per ciascun client il ***Nome host***, l'***Indirizzo MAC*** e l'***Indirizzo IP***. Sono disponibili, inoltre, le informazioni sul ***Tempo di attività*** aggiornate al momento della connessione in corso di ciascun client della rete locale.

- ***Ripetitore (WDS)***
  - ***Stato***

    Visualizza lo stato del WDS (Wireless Distribution System) della rete wireless per aumentare la portata.
  - ***Link WDS***

    Visualizza il numero delle connessioni correnti ad altri punti di accesso o Repeater della rete wireless.

➞ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Dispositivo

Alla pagina ***Dispositivo*** nel menu ***Stato*** sono disponibili informazioni sui dati importanti dell'apparecchio.

- ***Intervallo di attività del sistema***
  Visualizza l'autonomia dell'apparecchio dall'ultimo avvio.
- ***Orario del sistema***
  Visualizza l'ora del sistema dell'apparecchio.
- ***Versione del firmware***
  Visualizza la versione del firmware installato sull'apparecchio.
- ***Versione bootcode***
  Visualizza la versione del codice di avvio installato al momento sull'apparecchio.
- ***Versione driver wireless***
  Visualizza la versione del driver WLAN installato al momento sull'apparecchio.
- ***Versione interfaccia utente***
  Visualizza la versione dell'interfaccia utente installata attualmente nel dispositivo.
- ***Versione hardware***
  Visualizza la versione hardware del proprio dispositivo.
- ***Numero di serie***
  Visualizza il numero di serie del proprio dispositivo.
- ***System Log***
  Il registro eventi di sistema è in grado di indicare importanti informazioni sulla funzioni dell'apparecchio e sui possibili problemi. È possibile adattare alle proprie esigenze il grado di complessità del registro eventi di sistema (vedere capitolo “System Log“ a pagina 85).

➙ Fare clic su ***Aggiorna*** per caricare di nuovo questa pagina e aggiornare i dati visualizzati.

Appendice

Disattivazione del proxy HTTP e configurazione del blocco dei popup

Per poter avviare il programma di configurazione, può essere necessario disattivare il proxy http del browser. Se si utilizza Windows Vista o Windows XP Service Pack 2, è necessario configurare il blocco dei popup. Entrambe le procedure sono descritte qui di seguito.

Disattivazione del proxy HTTP

Assicurarsi che il Proxy HTTP del browser sia disattivato. Questa funzione deve essere disattivata in modo che il browser possa accedere alle pagine di configurazione del Gigaset SE366 WLAN.

Nella descrizione seguente viene indicata la procedura per Internet Explorer e Mozilla Firefox. Definire poi quale browser utilizzare e seguire i passi relativi.

- **Internet Explorer**

➡ Aprire Internet Explorer e fare clic nel menu ***Opzioni*** sulla voce ***Opzioni Internet***.

➡ Nella finestra ***Opzioni Internet*** aprire la scheda ***Connessioni***.

➡ Fare clic su ***Impostazioni LAN***.

➡ Disattivare tutte le opzioni della finestra ***Impostazioni LAN***.

➡ Fare clic su ***OK*** e di nuovo su ***OK*** per chiudere la finestra ***Opzioni Internet***.

- **Mozilla Firefox**

➡ Aprire Mozilla Firefox. Fare clic su ***Strumenti*** quindi su ***Impostazioni***.

➡ Nella finestra ***Impostazioni*** fare clic su ***Preferenze di connessione...***

➡ Nella finestra ***Impostazioni di connessione*** selezionare l'opzione ***Connessione diretta a Internet***.

➡ Terminare con ***OK***.

Configurazione del blocco dei popup

È necessario consentire i popup per il programma di configurazione per poterlo avviare.

◆ **Internet Explorer**

Se si lavora con Windows XP Service Pack 2, i popup di norma sono bloccati. Procedere come segue:

➥ Fare clic con il tasto destro del mouse sulla barra delle informazioni del browser.

➥ Selezionare ***Consenti popup nella pagina corrente***.

➥ Confermare la finestra di dialogo con ***OK***.

Vengono quindi consentite le pagine di configurazione del Gigaset SE366 WLAN come popup.

È possibile eseguire ulteriori impostazioni relative al comportamento di Internet Explorer riguardo ai popup selezionando la voce di menu ***Strumenti – Popup-Manager*** oppure con ***Strumenti – Opzioni Internet*** sulla scheda***Protezione*** .

◆ **Mozilla Firefox**

I popup sono normalmente bloccati. Procedere come segue:

➥ Aprire Mozilla Firefox. Fare clic su ***Strumenti*** quindi su ***Impostazioni***.

➥ Nella finestra ***Opzioni*** aprire la scheda ***Proprietà Web***.

➥ Disattivare nella finestra ***Proprietà Web*** l'opzione ***Blocca finestre pop-up***.

➥ Terminare con ***OK***.

Avvertenza:
Qualora si utilizzi un blocco dei popup diverso, è necessario configurarlo come necessario.

Ricerca errori

In questo capitolo vengono descritti i problemi più comuni e le relative soluzioni. Il Gigaset SE366 WLAN può essere controllato facilmente con l'ausilio dei LED luminosi presenti sull'apparecchio. In questo modo è possibile riconoscere rapidamente i problemi. Se non si riescono a risolvere problemi di connessione dopo aver controllato i LED luminosi, vedere nelle altre sezioni della tabella successiva.

Problema	**Possibile causa e interventi per eliminarla**
La spia di esercizio Power non si accende.	Mancanza di alimentazione elettrica. ➔ Verificare se l'alimentatore·è collegato al Gigaset SE366 WLAN e alla presa elettrica. ➔ Verificare se la presa di corrente e l'alimentatore funzionano. In caso di alimentatore difettoso, rivolgersi al servizio clienti (v. pag. 106).
Il LED della LAN di un apparecchio collegato non si accende.	Nessuna connessione LAN ➔ Verificare che l'apparecchio collegato sia acceso. ➔ Verificare se il cavo Ethernet è inserito. ➔ Controllare se si utilizza il tipo di cavo giusto (CAT 5) e che il cavo non sia più lungo di quanto permesso (<100 m). ➔ Verificare la possibile presenza di difetti sulla scheda di rete dell'apparecchio collegato e dei cablaggi. Eventualmente sostituire la scheda di rete difettosa oppure il cavo difettoso. ➔ Nella Gestione Periferiche di Windows (***Risorse del computer*** – ***Proprietà***), controllare se la scheda di rete è operativa. Se compare una croce di colore rosso oppure un punto interrogativo, è possibile che il driver non sia installato oppure che siano presenti conflitti di risorse. Seguire le indicazioni di Windows per risolvere il problema.

Problema	Possibile causa e interventi per eliminarla
Non è possibile stabilire una connessione a Internet.	➞ Verificare che l'opzione ***Connessione su richiesta*** sia disattivata. In questo caso non è possibile stabilire automaticamente le connessioni. ➞ Scegliere ***Connessione su richiesta***. ➞ La connessione è stata terminata manualmente con l'opzione ***Connessione su richiesta*** attivata. – Ristabilire la connessione manualmente con il pulsante ***Connetti*** oppure – riavviare il Gigaset SE366 WLAN. In entrambi i casi è valida l'impostazione per ***Connessione su richiesta***. ➞ Verificare se sono inseriti i dati di accesso corretti del proprio operatore. ➞ Possibilmente c'è un problema da parte dell'operatore. Prendere contatto con l'operatore.
Non avviene alcuna connessione dell'apparecchio con collegamento wireless al Gigaset SE366 WLAN.	Si sta tentando di eseguire nell'adattatore di rete una registrazione WPS ma il tasto di registrazione del Gigaset SE366 WLAN non è stato premuto. ➞ Premere il tasto di registrazione sul retro del Gigaset SE366 WLAN e attivare WPS entro due minuti nell'adattatore di rete. Per la registrazione WPS si è stabilito un PIN ma l'adattatore di rete non usa un PIN o non usa quello corretto. ➞ Controllare le impostazioni per la crittografia della rete wireless e controllare quale sia il PIN usato dal Gigaset SE366 WLAN. Digitare tale PIN nell'adattatore di rete. L'adattatore di rete wireless non utilizza l'SSID corretto. ➞ Modificare l'SSID nell'adattatore di rete o usare WPS. Sono stati impostati SSID e crittografia a mano, ma poi si è eseguita una registrazione WPS. ➞ Controllare quali siano l'SSID e la Pre-shared Key usati e configurare con essi i client WLAN. È stato attivato il controllo di accesso tramite filtri MAC ma il PC non è compreso nella lista degli indirizzi MAC. ➞ Inserire il PC che intende registrarsi tramite WPS nella lista degli indirizzi MAC.

Problema	Possibile causa e interventi per eliminarla
Dopo aver tentato una registrazione WPS, il LED **WLAN** continua a lampeggiare e il client desiderato non è registrato.	Più di un client ha tentato di registrarsi. ➞ Controllare se eventualmente un apparecchio estraneo si è registrato nella WLAN. Se sì: ➞ modificare immediatamente la chiave WPA-PSK a mano (v. pag. 69) ed effettuare la registrazione WPS dei client con PIN (v. pag. 68). Se no: ➞ ritentare la registrazione dopo un breve tempo
Non avviene alcuna connessione dell'apparecchio con collegamento wireless al Gigaset SE366 WLAN.	Nel Gigaset SE366 WLAN è attivata una crittografia ma non nell'adattatore wireless oppure non utilizza la chiave corretta oppure utilizza un altro tipo di crittografia. ➞ Attivare nell'adattatore di rete la stessa crittografia con la chiave corretta o usare WPS. Se non si conosce la chiave è necessario reimpostare il Gigaset SE366 WLAN (v. pag. 20). **Avviso**: Tenere conto che in tal modo sono state reimpostate **tutte** le impostazioni di configurazione sulle impostazioni iniziali. La funzione ***Rete wireless*** è disattivata. ➞ Controllare se la funzione ***Rete wireless*** è disattivata ed attivarla (v. pag. 65). Nel PC manca la connessione wireless alla rete. ➞ Nella Gestione Periferiche di Windows (***Risorse del computer*** – ***Proprietà***), controllare se la connessioni di rete è operativa. Se compare una croce di colore rosso oppure un punto interrogativo, è possibile che il driver non sia installato oppure che siano presenti conflitti di risorse. Seguire le indicazioni di Windows per risolvere il problema.

Problema	Possibile causa e interventi per eliminarla
Il Gigaset SE366 WLAN oppure altri PC non possono essere raggiunti da un PC della LAN collegata con il comando **ping**.	➔ Assicurarsi che su tutti i PC della rete locale sia installato e configurato TCP/IP. ➔ Verificare se gli indirizzi IP sono configurati correttamente. Nella maggior parte dei casi è possibile utilizzare la funzione DHCP del Gigaset SE366 WLAN, per attribuire indirizzi dinamici ai PC nella LAN. In questo caso per tutti i PC, nelle impostazioni TCP/IP della configurazione di rete è necessario stabilire che ottengano automaticamente l'indirizzo IP. Se gli indirizzi IP vengono configurati manualmente nella LAN, è importante ricordare che bisogna utilizzare la maschera di sottorete 255.255.255.x. Ciò significa che le prime tre parti dell'indirizzo IP su ciascun PC e sul Gigaset SE366 WLAN devono essere identiche. L'apparecchio deve essere, inoltre, configurato come server DNS.
Nessuna connessione con l'interfaccia operativa del Gigaset SE366 WLAN	➔ Verificare con il comando **ping** se è possibile creare una connessione di rete al Gigaset SE366 WLAN. ➔ Controllare il cavo di rete tra il PC da cui si desidera gestire l'apparecchio e il Gigaset SE366 WLAN. ➔ Se il PC da cui si desidera gestire l'apparecchio si trova nella rete locale del router, assicurarsi di utilizzare la gestione indirizzi IP corretta (vedere sopra). ➔ Se il PC da cui si desidera gestire l'apparecchio non si trova nella rete locale del router deve essere autorizzato dalla gestione remota.
Password dimenticata oppure persa.	➔ Reimpostare il Gigaset SE366 WLAN (v. pag. 21). **Avviso**: Tenere conto che in tal modo sono state reimpostate **tutte** le impostazioni di configurazione sulle impostazioni iniziali.
Non è possibile accedere a una risorsa (unità o stampante) su un altro PC	➔ Assicurarsi che su tutti i PC della rete locale sia installato e configurato TCP/IP e che i PC appartengano tutti allo stesso gruppo di lavoro. ➔ Verificare se la risorsa sul relativo PC è stata rilasciata e se si possiedono i diritti di accesso necessari. ➔ Stampa: verificare se la stampante è impostata come stampante di rete.

Problema	Possibile causa e interventi per eliminarla
La velocità di trasmissione è troppo bassa. Si hanno ad esempio errori di Pixel nel Video-Streaming.	➞ La trasmissione dati via radio dipende dalle condizioni ambientali, ad.esempio dalla struttura dell'edificio o da influenze di altri apparecchi vicini che emettono nella banda di 2,4 GHz. ➞ Collare gli apparecchi WLAN in modo da avvicinarli. ➞ Modificare l'orientamento dell'antenna. ➞ Collocare l'apparecchio in un luogo diverso. ➞ Spegnere le altre frequenze radio presenti nell'ambiente. Esse possono disturbare la trasmissione dei dati. ➞ Provare con un canale diverso. ➞ Controllare se il problema esiste anche con un altra modalità di crittografia.

Funzioni del Gigaset SE366 WLAN e loro interdipendenze

La seguente tabella mostra quali funzioni dell'apparecchio siano possibili in determinate combinazioni. In caso di errore controllare le seguenti condizioni:

Funzione	**possibile in combinazione con**	**non possibile in combinazione con**
WPS	WPA2-PSK / WPA-PSK Crittografia	Autenticazione WPA2 / WPA Crittografia WEP
Modalità di trasmissione IEEE 802.11n	WPA2-PSK / WPA-PSK Crittografia	Autenticazione WPA2 / WPA Crittografia WEP
WDS	Crittografia WEP (fino a 6 connessioni WDS) WPA2-PSK/WPA-PSK-Crittografia (una connessione WDS)	WPA2/WPA

Specifiche

Interfacce

1 Modem	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
4 LAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
WLAN	IEEE 802.11n (Draft, vedi v. pag. 15), per il collegamento wireless di massimo 32 PC

Proprietà radio

Gamma di frequenze	da 2.400 a 2.484 GHz banda ISM
Spreading	Direct Sequence Spread Spectrum (DSSS)
Modulazione	CCK, OFDM
Numero di canali	13: tutti i paesi escluso Giappone, USA e Canada) 11: USA e Canada
Velocità di trasmissione	IEEE 802.11b: fino a 11 Mbps IEEE 802.11g: fino a 54 Mbps IEEE 802.11n (Draft, vedi v. pag. 15): fino a 300 Mbps
Portata	ca. 50 m negli spazi chiusi, fino a 300 m all'aperto
Design dell'antenna	3*3, dualband

Ambiente operativo

Temperatura	Temperatura di esercizio da 0 °C a 40 °C Temperatura di stoccaggio da -20 a 70 °C
Umidità dell'aria	5 % - 90 % (senza condensa)
Spie LED	Power Online (Internet) WLAN (attività, wireless, registrazione WPS) WAN (connessione a modem, attività) LAN1... LAN4 (connessione al PC, attività, via cavo)

Rispetto delle condizioni di sicurezza e delle norme

CE, EN60950
Anatel (previsto)

Software	Interfaccia di configurazione basata su browser NAT, PPPoE Server e client DHCP NAT, Port-Forwarding, Port-Triggering, Exposed Host Setup di protezione Firewall, ostacolo agli attacchi hacker Filtro indirizzo MAC Filtro URL, DoS-Blocking, SPI Crittografia WPA2-PSK / WPA-PSK Crittografia WPA2 / WPA Crittografia WEP WPS (Wi-Fi Protected Setup), 1click only Configurazione LAN WDS

CONFORMITÀ CE

Con la presente Gigaset Communications GmbH dichiara che questo terminale è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla Direttiva 1999/05/CE.

Questo apparecchio è previsto per l'impiego in tutto il mondo, al di fuori della Comunità Economica Europea (con eccezione della Svizzera) dipendentemente dalle omologazioni nazionali.

In Francia questo apparecchio è previsto solo per l'uso all'interno di edifici.

Ogni requisito specifico del Paese è stato tenuto in debita considerazione.

Copia della dichiarazione CE di conformità, redatta ai sensi della Direttiva 1999/05/CE, è disponibile al seguente indirizzo Internet:
www.gigaset.com/docs

Cliccando ancora su "Declarations of Conformity" nell'area Customer Care, troverete quanto cercate oppure è possibile richiederla telefonando al Servizio Clienti.

CE 0682 !

Smaltimento

Italia

INFORMAZIONE AGLI UTENTI

Eco-contributo RAEE assolto ove dovuto - N° Iscrizione Registro A.E.E.: IT08010000000060.

Ai sensi dell'art 13 del Decreto Legislativo 25 luglio 2005, n. 151 "Attuazione delle Direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti".

Il simbolo del cassonetto barrato riportato sull'apparecchiatura indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

L'utente dovrà, pertanto, conferire l'apparecchiatura giunta a fine vita agli idonei centri di raccolta differenziata dei rifiuti elettrici ed elettronici, oppure riconsegnarla al rivenditore al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente, in ragione di uno a uno.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte dell'utente comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente. Gli utenti professionali dovranno farsi carico di concordare l'attività di smaltimento del prodotto a fine vita. Fare riferimento anche al sito www.gigaset.com/it "Area Ambiente" direttiva RAEE.

Svizzera

Nota concernente il riciclaggio

Questo apparecchio non deve in nessun caso essere eliminato a traverso la spazzatura normale alla fine della propria funzione. Si deve invece portare o ad un punto di vendita oppure ad un punto di smaltimento per apparecchi elettrici e elettronici secondo l'ordinanza concernente la restituzione, la ripresa e lo smaltimento degli apparecchi elettrici ed elettronici (ORSAE).
I materiali sono riutilizzabili secondo la propria denominazione. Con la riutilizzazione, o tutt' altro impiego di questi materiali, contribuite in maniera importante alla protezione dell' ambiente.

Servizio Clienti (Customer Care) (Italia)

Per informazioni sulla situazione di eventuali riparazioni in corso, sui centri di assistenza, per informazioni commerciali o relative all'uso del terminale potete rivolgervi al Servizio Clienti chiamando il numero unico da tutta Italia dalle ore 09.00 alle ore 18.00 dal lunedì al venerdì e dalle ore 09.00 alle ore 13.00 il sabato:

Servizio Clienti Italia

Tel. 199.15.11.15

Il servizio offerto è a tariffa unica da tutta Italia in qualunque fascia oraria.

Il numero può essere chiamato da qualunque operatore di rete fissa o mobile.

Il costo della chiamata effettuata da telefoni fissi della rete Telecom Italia è di €cent 8,36 + IVA al minuto mentre per le chiamate effettuate attraverso la rete di altri operatori consultate le tariffe offerte dall'operatore stesso.

Il costo di ogni comunicazione verrà calcolato sulla base della sua effettiva durata misurata in secondi senza scatto alla risposta.

Il Servizio Clienti è contattabile anche via e-mail entrando nel sito:

www.gigaset.com/it

cliccando poi su "Contatti". Vi apparirà un modulo da compilare, riceverete risposta nel più breve tempo possibile.

Se il prodotto non è venduto da rivenditori autorizzati sul territorio nazionale potrebbe non essere totalmente compatibile con la rete telefonica nazionale. Se l'apparato è stato progettato per essere usato in Italia è chiaramente riportato in lingua Italiana sia sulla scatola accanto al marchio CE che serigrafato in modo indelebile sotto la stazione base. Se l'apparato viene comunque usato in modo non conforme alle indicazioni riportate sul manuale e sul prodotto stesso, potrebbero non sussistere le condizioni per godere dei diritti all'assistenza ed alla riparazione sia in garanzia che fuori garanzia.

Servizio Clienti (Customer Care) (Svizzera)

Vi offriamo una consulenza rapida e personalizzata!

Il nostro supporto in linea in Internet è raggiungibile sempre e dappertutto:
www.gigaset.com/customercare
Per 24 ore su 24 avete a disposizione il supporto sui nostri prodotti. Vi trovate una raccolta delle domande poste più di frequente con relative risposte, nonché i manuali d'istruzione e gli aggiornamenti del software (se disponibili per il prodotto in questione) da scaricare.

Le domande poste più di frequente con relative risposte si trovano anche nell'appendice delle presenti istruzioni d'uso.

Una consulenza personale sulla nostra offerta è disponbile con la Premium-Hotline:

Svizzera 0848 212 000 (0,08 SFr./Min.)

Vi attendono collaboratori qualificati che vi aiutano con competenza relativamente alle informazioni sui prodotti e sulla loro installazione.

Nel caso della necessità di una riparazione o di eventuali richieste di garanzia, otterrete un aiuto rapido ed affidabile presso il nostro Service-Center.

Svizzera 0848 212 000 (0,08 SFr./Min.)

Tenete a portata di mano la prova d'acquisto.

Nei Paesi nei quali il nostro prodotto non viene venduto tramite distributori autorizzati, non vengono offerti servizi di sostituzione o riparazione.

Open Source Software

The Gigaset SE366 WLAN contains, among other things, Open Source Software, which is licensed under the GNU General Public License and the GNU Lesser General Public License. This Open Source Software was developed by third parties and is protected by copyright. The license texts in the original English version are provided on the next pages.

The software is made available free of charge. You are entitled to use this Open Source Software as foreseen in the above-mentioned license conditions. In the event of conflicts between these license conditions and the Gigaset Communications GmbH license conditions for the software, the above-mentioned license conditions shall prevail with respect to the Open Source Software.

The GNU General Public License (GPL) is supplied with this product. In addition, you can download the license conditions from the Internet.

- You will find the GPL on the Internet at:
  http://www.gnu.org/copyleft/gpl.html
- The source text including copyright notices of the Open Source Software can be found on the Internet at:
  http://www.gigaset.com/developer

If not already supplied with the product, you can request the source text including copyright notices from Gigaset Communications GmbH by paying a fee to cover the physical act of transferring the copy. Requests can be submitted by e-mail or fax to the address or fax number below within three years of purchase of this product, indicating the precise device type as well as the version number of the installed device software.

Kleinteileversand Bocholt

E-Mail: kleinteileversand.com@gigaset.com

Fax: + 49 2871 / 91 30 29

Gigaset Communications GmbH provides no warranty for the Open Source Software contained in this product if used in any manner other than the program execution intended by Gigaset Communications GmbH. The GNU General Public License defines the warranty for defects, if any, from the author or other licensors of the Open Source Software.

Gigaset Communications GmbH specifically disclaims any warranties for defects against it if a product defect is or could have been caused by altering any Open Source Software program or the product's configuration. In addition, you have no warranty claims against Gigaset Communications GmbH in the event that the Open Source Software infringes the intellectual property rights of a third party.

Technical support shall only be provided by Gigaset Communications GmbH for the software including the Open Source Software portion contained within, if this software has not been modified.

Glossario

Adattatore di rete

L'adattatore di rete è l'hardware che effettua il collegamento di un componente di rete alla rete locale. Il collegamento può, quindi, avvenire wireless oppure via cavo. Un adattatore di rete via cavo è per es. una scheda di rete Ethernet. Gli adattatori di rete wireless sono per es. la Gigaset PC Card 300 e il Gigaset USB Adapter 300.

Un adattatore di rete ha un indirizzo univoco, l'Indirizzo MAC.

Area IP-Pool

Nel pool di indirizzi IP del Gigaset SE366 WLAN è definita un'area di Indirizzo IP che può utilizzare il Server DHCP del router per assegnare Indirizzo IP dinamico.

Attacco DoS

Denial of Service

Un attacco DoS è una forma particolare di attacco hacker indirizzato contro computer e reti con connessione a Internet. Lo scopo non è proprio di rubare dati ma piuttosto di indebolire il computer o la rete in modo che non siano più disponibili le risorse di rete. Per esempio, un tipico attacco hacker consiste nel fatto che un computer remoto rende noto che lavora per conto del computer indebolito e riceve determinati dati per conto dell'utente.

Beacon

I beacon sono pacchetti informativi inviati dagli apparecchi di una rete wireless a tutti gli altri apparecchi per segnalare la loro disponibilità e capacità di ricevere. I beacon servono inoltre a sincronizzare le reti wireless. Un intervallo di beacon è il tempo tra due beacon in millisecondi.

Bridge

Un Bridge collega più segmenti di rete a una rete completa, per es. a una rete TCP/IP. I segmenti possono avere proprietà fisiche diverse, per es. cablaggi diversi come in Ethernet e LAN wireless. Attraverso la combinazione di singoli segmenti di rete tramite bridge, le reti locali possono essere estese praticamente senza limiti.

Vedere anche: Switch, Hub, Router, Gateway

Broadcast

Un Broadcast è un pacchetto dati che non è indirizzato a un determinato destinatario ma a tutti i componenti di rete di una rete. Il Gigaset SE366 WLAN non inoltra i pacchetti Broadcast a Internet, essi restano sempre all'interno della rete locale (LAN) che viene gestita dal Gigaset SE366 WLAN.

BSSID

Basic Service Set ID

L'BSSID serve a distinguere in modo univoco una rete wireless (WLAN) da un'altra. In Modalità infrastruttura il BSSID è l'Indirizzo MAC del Punto di accessos. Nelle reti wireless in Modalità ad hoc il BSSID è l'indirizzo MAC di un qualsiasi partecipante.

Client

Un Client è un'applicazione che richiede un servizio a un server. Per esempio un client HTTP chiede a un PC della rete locale dati, ovvero pagine web, di un server HTTP in Internet. Spesso i componenti di rete vengono (ad es. il PC), su cui è operativa l'applicazione client, definiti ugualmente come client.

Connessione se necessario

Connessione se necessario significa che le applicazioni come per es. il browser, Messenger ed e-mail stabiliscono un collegamento automatico a Internet quando vengono avviate. Ciò può causare elevati costi di connessione se non si utilizza una Tariffa flat. Questa funzione può essere attivata nel Gigaset SE366 WLAN per ridurre i costi.

Crittografia

La crittografia serve a proteggere informazioni riservate dagli attacchi non autorizzati. Con l'ausilio di un sistema di crittografia i pacchetti dati vengono inviati in modo sicuro lungo la rete. Il Gigaset SE366 WLAN offre per la trasmissione sicura dei dati in rete wireless la crittografia WEP e WPA.

DHCP

Dynamic Host Configuration Protocol

Il protocollo DHCP regola l'immissione automatica di Indirizzo IP nei componenti di rete. È stato sviluppato poiché nelle grandi reti, in particolare in Internet, stabilire gli indirizzi IP è molto complesso dato che i partecipanti spesso cambiano, si disconnettono o aumentano. Un server DHCP assegna ai componenti di rete collegati (DHCP-Clients) di un Area IP-Pool stabilito in modo automatico Indirizzo IP dinamico facendo risparmiare molto tempo di configurazione. Inoltre, i campi di indirizzi vengono utilizzati in modo più efficace: poiché tutti i partecipanti non sono attivi contemporaneamente in rete, secondo le esigenze, è possibile immettere lo stesso indirizzo IP in sequenza nei diversi componenti di rete.

Il Gigaset SE366 WLAN include un server DHCP e può, quindi, assegnare gli indirizzi IP in modo automatico ai PC della rete locale. Perciò è possibile stabilire per PC speciali che i relativi indirizzi IP non vengano mai cambiati.

DMZ

Demilitarized Zone, vedi anche Exposed Host

DMZ definisce l'ambito di una rete che si trova all'esterno del Firewall. Una DMZ viene impostata per così dire tra una rete da proteggere (per es. una LAN) e una rete non sicura (ad es. Internet). Una DMZ è utile se si desidera offrire in Internet servizi Server che, per motivi di sicurezza, non devono operare all'interno del firewall oppure se le applicazioni Internet non funzionano correttamente dietro un firewall. Una DMZ consente l'accesso illimitato da Internet solo a uno o pochi componenti di rete mentre gli altri componenti di rete restano al sicuro dietro il firewall.

DNS

Domain Name System

DNS consente di associare ai PC o ai Nome di dominio indirizzi IP più facili da ricordare. Per ciascuna LAN con collegamento Internet un server DNS deve gestire queste informazioni. Appena viene scelta una pagina in Internet, il browser preleva l'indirizzo IP da corrispondente server DNS per stabilire la connessione.

In Internet l'assegnazione del nome di dominio agli indirizzi IP avviene in un sistema suddiviso in modo gerarchico. Un PC locale conosce solo l'indirizzo del server locale. Questo conosce tutti gli indirizzi dei computer nella rete locale, nonché i server superiori, che conoscono indirizzi o altri nomi di server superiori.

DSL

Digital Subscriber Line

DSL è una tecnica di trasmissione di dati con cui l'accesso a larga banda a Internet può essere eseguito tramite la linea telefonica comune. La porta DSL viene fornita da un Operatore di rete. Per funzionare è necessario un modem DSL.

DTIM

Delivery Traffic Indication Message

Un DTIM è un segnale che viene inviato da un punto di accesso quale parte di un Beacon ad un apparecchio client nella modalità di risparmio energetico per segnalargli che deve essere consegnato un pacchetto di dati. L'l'intervallo DTIM stabilisce la frequenza con la quale un DTIM è presente in una serie di pacchetti beacon.

Duplex

Modalità di trasmissione dati, in cui è possibile inviare e ricevere contemporaneamente.

Vedi anche Semiduplex

DynDNS

DNS dinamico

La correlazione di Nome di dominio e Indirizzo IP viene realizzata tramite il Domain Name Service (DNS). Per l'Indirizzo IP dinamico questo servizio viene integrato dal cosiddetto Dynamic DNS (DynDNS). Consente l'utilizzo di un componente di rete con indirizzo IP dinamico come Server in Internet. DynDNS assicura che un servizio in Internet può essere raggiunto indipendentemente dall'indirizzo IP corrente sempre sotto lo stesso nome di dominio.

Ethernet

Ethernet è una tecnologia di rete per le reti locali (LANs) ed è stata definita da IEEE quale standard IEEE 802.3. Ethernet utilizza per la trasmissione di dati un cavo baseband con velocità di trasmissione di 10 oppure 100 Mbps.

Exposed Host

Exposed Host si riferisce a un PC che si trova al di fuori del firewall.

Vedi anche DMZ

Firewall

Con un firewall i gestori di rete si proteggono dagli accessi non autorizzati. Si tratta, quindi, di un insieme di misure e tecniche sotto forma di hardware e/o software che controllano il flusso di dati tra una rete privata da proteggere e una rete non protetta come Internet.

Vedi anche NAT

Gateway

Un gateway è un apparecchio che collega reti con architetture completamente diverse (indirizzamento, protocolli, interfaccia utente, ecc.). Anche se non è propriamente corretto, il concetto viene spesso utilizzato con lo stesso significato di Router.

Vedi anche Bridge, Hub, Router, Switch

Gestione remota

Gestione remota si riferisce alla possibilità di amministrare una rete da un componente di rete che si trova al di fuori della rete locale (LAN).

Hub

Un hub collega più componenti di rete tra di loro in una rete con topologia a stella inoltrando tutti i dati ricevuti da uno dei componenti di rete a tutti gli altri.

Vedi anche Switch, Bridge, Router, Gateway

IEEE

Institute of Electrical and Electronic Engineers

L'IEEE è un comitato internazionale che stabilisce le norme in ambito di reti, in particolare per la standardizzazione di tecnologie, protocolli di trasmissione, velocità di trasmissione di dati e connessione LAN.

IEEE 802.11

IEEE 802.11 è uno standard per LAN radio in banda di 2.4 GHz. Gli apparecchi finali possono essere collegati nella cosiddetta Modalità infrastruttura con una stazione base (Punto di accesso) oppure possono stabilire connessioni spontanee tra di loro (Modalità ad hoc).

IGMP

Internet Group Management Protocol

IGMP è un Protocollo Internet che consente a un computer in Internet di notificare ai router adiacenti la propria appartenenza al gruppo multicast. Con il multicasting un computer può inviare contenuto a diversi altri computer che hanno dimostrato interesse al contenuto del computer originale. Il multicasting può essere utilizzato, per esempio, per i programmi multimediali per il Media Streaming a destinatari che hanno impostato una appartenenza in un gruppo multicast.

Indirizzo IP

L'indirizzo IP è un indirizzo univoco su tutta la rete di un componente di rete in una rete sulla base dei protocolli TCP/IP (ad es. in una rete locale (LAN) oppure in Internet). L'indirizzo IP è composto da quattro blocchi numerici (valori da 0 a 255) separati da un punto (ad es. 192.168.1.1). L'indirizzo IP è composto dall'indirizzo della rete e dall'indirizzo del PC. A seconda della Subnetz mask uno, due o tre blocchi numerici compongono l'indirizzo di rete, il resto è costituito dall'indirizzo del PC. L'indirizzo IP del PC è disponibile digitando **`ipconfig`** nel prompt dei comandi.

Gli indirizzi IP possono essere assegnati manualmente (vedere Indirizzo IP statico) oppure automaticamente (vedere Indirizzo IP dinamico).

In Internet invece degli indirizzi IP vengono utilizzati di norma i Nome di dominio. La correlazione tra nomi di dominio e indirizzi IP viene effettuata dal DNS.

Il Gigaset SE366 WLAN ha un Indirizzo IP privato e un Indirizzo IP pubblico.

Indirizzo IP globale

Vedi Indirizzo IP pubblico

Indirizzo IP dinamico

Un Indirizzo IP dinamico viene assegnato a un componente di rete automaticamente tramite DHCP. In tal modo, l'indirizzo IP cambia a ogni connessione o a determinati intervalli di tempo.

Vedi anche Indirizzo IP statico

Indirizzo IP locale

Vedi Indirizzo IP privato

Indirizzo MAC

L'indirizzo MAC serve per l'identificazione a livello mondiale di un Adattatore di rete. È composto da sei parti (numeri esadecimali, per es. 00-90-96-34-00-1A. L'indirizzo MAC viene assegnato dalla casa produttrice dell'adattatore di rete.

Indirizzo IP privato

L'Indirizzo IP privato (anche indirizzo IP locale) l'indirizzo di un componente di rete in rete locale (LAN). Può essere assegnato a piacere dall'Operatore di rete. Gli apparecchi che vengono utilizzati ai fini di una connessione di una rete locale come il Gigaset SE366 WLAN hanno un indirizzo IP privato e un Indirizzo IP pubblico.

Indirizzo IP pubblico

L'Indirizzo IP pubblico (anche indirizzo IP globale) l'indirizzo di un componente di rete in Internet. Viene assegnato dall'Operatore di rete. Gli apparecchi che creano una connessione di rete locale a Internet, come il Gigaset SE366 WLAN, hanno un indirizzo IP pubblico e un Indirizzo IP privato.

Indirizzo IP statico

Un Indirizzo IP statico viene assegnato a un componente di rete manualmente durante la configurazione di rete. Diversamente dall'Indirizzo IP dinamico, l'indirizzo IP statico non cambia.

Media Access Control

Internet

Internet è una cosiddetta (WAN) (Wide Area Network) che comprende globalmente diversi milioni di partecipanti. Per lo scambio dei dati è stata definita una serie di Protocollo raggruppati sotto il nome di TCP/IP. Tutti i partecipanti collegati a Internet sono identificabili attraverso un Indirizzo IP. Ai server si accede attraverso il Nome di dominio (ad es. gigaset.com). La correlazione tra i nomi di dominio e gli indirizzi IP viene eseguita dal Domain Name Service (DNS).

Tra i servizi più importanti di Internet vi sono:

- la posta elettronica (eMail)
- il World Wide Web (WWW)
- il trasferimento file (FTP)
- i forum di discussione (Usenet / Newsgroups)

Intervallo di rekey

L'intervallo di rekey è un lasso di tempo dopo il quale per la crittografia dei dati con WPA-PSK viene generata automaticamente una nuova chiave.

ISP

Internet Service Provider, vedi Operatore di rete

IP

Internet Protocol

Il Protocollo IP appartiene ai protocolli TCP/IP. Serve all'indirizzamento dei partecipanti di una rete sulla base degli Indirizzo IP e comunica i dati di un mittente al destinatario. In questo modo stabilisce l'instradamento per i pacchetti di dati tra il mittente e il destinatario in una rete complessa (routing).

LAN

Local Area Network = rete locale

Una rete locale è una concentrazione di componenti di rete finalizzata allo scambio di dati e all'utilizzo di risorse comuni. L'estensione spaziale è limitata a una zona determinata (un terreno). Di norma utenti e gestori sono identici. Una rete locale può essere collegata con altre reti locali oppure con una rete a estensione geografica (WAN) come Internet.

Mediante Gigaset SE366 WLAN è possibile impostare una rete locale via cavo Ethernet e una rete standard wireless IEEE 802.11n (WLAN).

Mbps

Million Bits per Second

Dato che indica la velocità di trasmissione in una rete.

MER

MAC Encapsulated Routing

Forma speciale di un protocollo di trasmissione per Internet.

Modalità ad hoc

La modalità ad hoc è una modalità operativa delle reti locali wireless (WLAN), dove i componenti di rete costituiscono una rete spontanea senza Punto di accesso, per es. più notebook in una conferenza. Tutti i componenti di rete hanno gli stessi diritti. Devono essere dotati di un Adattatore di rete wireless.

Modalità infrastruttura

La modalità infrastruttura è una modalità operativa delle reti wireless locali (WLAN), in cui il Punto di accesso regola il traffico di dati. I componenti di rete non possono, quindi, stabilire alcun collegamento diretto tra di loro come in Modalità ad hoc.

MRU

Maximum Receive Unit

L'unità MRU definisce la quantità di dati massima all'interno di un pacchetto di dati.

MTU

Maximum Transmission Unit

L'unità MTU definisce la lunghezza massima di un pacchetto di dati da trasportare in una volta in rete.

NAT

Network Address Translation

Il NAT è un metodo per trasferire gli indirizzi IP (in genere Indirizzo IP privaton) in una rete su uno o più Indirizzo IP pubblico in Internet. Con il metodo NAT è possibile utilizzare più componenti di rete in una LAN insieme agli indirizzi IP pubblici di un router per l'accesso a Internet. I componenti di rete della rete locale vengono nascosti dietro gli indirizzi IP registrati in Internet del router. Mediante questa funzione di protezione il NAT viene spesso impostato come parte del Firewall di una rete. Per eseguire i servizi di un PC della rete locale nonostante il NAT in Internet, configurare il Gigaset SE366 WLAN come Server virtuale.

Nome di dominio

Il nome di dominio è la definizione di uno o più server Web in Internet, ad esempio gigaset.com. Il nome di dominio viene fatto corrispondere tramite il servizio DNS al corrispondente Indirizzo IP.

Operatore di rete

Un operatore di rete (Internet Service Provider) consente l'accesso dietro compenso a Internet.

Porta

Attraverso una porta vengono scambiati dati tra due applicazioni in rete. Il numero della porta si rivolge a un'applicazione all'interno dei componenti di rete. La combinazione Indirizzo IP/numero della porta identifica il destinatario o il mittente di un pacchetto di dati all'interno della rete in modo univoco. Alcune applicazioni (per es. servizi Internet quali HTTP oppure FTP) operano con numeri di porta statici, altri ricevono a ciascun accesso un numero di porta libero.

Port-Forwarding

Mediante il Port-Forwarding il Gigaset SE366 WLAN inoltra pacchetti di dati da Internet, indirizzati a una determinata Porta, alla porta corrispondente del relativo componente di rete. In tal modo i server della rete locale possono fornire i servizi in Internet senza bisogno di un Indirizzo IP pubblico.

Vedere anche: Server virtuale

PPPoA

Point-to-Point Protocol over ATM = protocollo punto-punto via ATM

Il PPPoA è un Protocollo per la connessione di componenti di rete di una rete locale Ethernet a Internet tramite rete ATM.

PPPoE

Point-to-Point Protocol over Ethernet = protocollo punto-punto via Ethernet

Il PPPoE è un Protocollo per la connessione di componenti di rete di una rete locale Ethernet a Internet tramite modem.

Protocollo

Un protocollo descrive le convenzioni per la comunicazione in una rete. Il protocollo contiene le regole per aprire, gestire e interrompere una connessione nonché informazioni sui formati dei dati, gli intervalli temporali e un'eventuale gestione degli errori. Per la comunicazione di due applicazioni sono necessari diversi protocolli a livelli diversi, per es. i protocolli TCP/IP in Internet.

Proxy HTTP

Un proxy HTTP è un Server mediante il quale i componenti di rete svolgono il proprio traffico Internet. Tutte le richieste vengono inviate tramite proxy.

Punto di accesso

Un punto di accesso, come per es. il Gigaset SE366 WLAN, è il centro di una rete locale wireless (WLAN). Fornisce la connessione dei componenti di rete collegati via radio e regola il traffico dei dati nella rete wireless. Il punto di accesso costituisce anche l'interfaccia per accedere ad altre reti, per es. a una LAN Ethernet esistente oppure con un modem in Internet. La modalità operativa delle reti wireless con punto di accesso è detta Modalità infrastruttura.

Rete

Una rete è un insieme di apparecchi collegati mediante diversi cavi o canali radio che condividono risorse comuni come dati e apparecchi periferici. Si distingue essenzialmente tra reti locali (LAN) e reti a estensione geografica (WAN).

Repeater

Un repeater amplia la portata di una rele locale wireless tramite l'inoltro dei dati dal Punto di accesso ad altri PC oppure Adattatore di rete.

Rete radio

Vedi WLAN

Roaming

Con il roaming aumenta la portata di una LAN wireless con l'impiego di più Punto di accesso che utilizzano lo stesso SSID e lo stesso canale radio e sono collegati tra di loro tramite Ethernet. I PC della rete possono cambiare in modo dinamico più punti di accesso senza perdere la connessione di rete esistente.

Router

Un router inoltra il pacchetto di dati da una rete locale (LAN) in un'altra e sceglie, quindi, la via più veloce. Un router consente il collegamento tra reti di diverse tecnologie di rete. Collega per esempio una rete locale con Ethernet oppure tecnologia WLAN con Internet.

Vedi anche Bridge, Switch, Hub, Gateway

Scadenza

La scadenza stabilisce il tempo durante il quale i PC assegnati dal server DHCP mantengono gli Indirizzo IP dinamico senza modificarli.

Semiduplex

Modalità operativa nella trasmissione di dati. Nello stesso momento è sempre possibile inviare o ricevere una pagina dati.

Vedi anche Duplex

Server

Un server fornisce un servizio ad altri componenti di rete (Clients). Di norma il concetto di server definisce un computer oppure un PC. Si può riferire anche soltanto a un'applicazione che fornisce un determinato servizio come il DNS oppure il servizio web.

Server DHCP

Vedi DHCP

Server DNS

Vedere DNS

Server RADIUS

Un server RADIUS funge da server di autenticazione centrale. Il server RADIUS si occupa in questo caso dell'autenticazione (controllo utente/password). Vengono però anche messi a disposizione i parametri per la connessione con il Client. Il server RADIUS preleva i dati a questo scopo utilizzati da propri file di configurazione, da propri database di configurazione o li rileva interrogando altri database o servizi di indici nei quali sono salvati i dati di accesso (ad esempio nome utente e password).

Server virtuale

Un Server virtuale fornisce un servizio in Internet che non funziona su di esso ma su un altro componente di rete. Il Gigaset SE366 WLAN può essere configurato come server virtuale. Esegue, quindi, l'inoltro di richieste provenienti dall'esterno a un servizio tramite il Port-Forwarding direttamente alla Porta corrispondente del relativo componente di rete della rete locale.

SMTP

Simple Mail Transfer Protocol

Il Protocollo SMTP appartiene alla famiglia di protocolli TCP/IP. Esso regola lo scambio di posta elettronica in Internet. A tale scopo, viene fornito quindi dall'Operatore di rete un server SMTP.

SNMP

Simple Network Management Protocol

Il Protocollo SNMP appartiene alla famiglia di protocolli TCP/IP. Offre un procedimento semplice per la gestione della rete fondato su una base di informazioni comuni per i dati di gestione e i messaggi di gestione della rete (cosiddetti Traps) e nella rete sotto controllo avvisa quando avviene un evento (ad es. allarme o notifica in caso di modifica di configurazione).

Sottorete

Una sottorete suddivide una rete in reti parziali più piccole.

SPI

Stateful Packet Inspection

Con SPI l'apparecchio controlla e limita l'accesso del traffico esterno da Internet. In tal modo è in grado di riconoscere e impedire determinati tipi di attacchi come per es. Denial-of-Service (DoS). Un tipico attacco DoS può consistere in un PC estraneo che indebolisce un sistema e funge da apparecchio indebolito per ricevere al suo posto i dati a questo inviati.

SSID

Service Set Identifier

L'SSID identifica le stazioni di una rete wireless (WLAN). Tutti i componenti di rete wireless che hanno lo stesso SSID costituiscono una rete comune. L'SSID può essere scelto liberamente.

Subnetz mask

La maschera di sottorete stabilisce quanti blocchi numerici dell'Indirizzo IP di una rete rappresentano l'indirizzo di rete e quanti l'indirizzo del computer.

La maschera di sottorete in una rete che viene gestita dal Gigaset SE366 WLAN è sempre 255.255.255.0. Questo significa che i primi tre blocchi numerici dell'indirizzo IP formano il numero della rete e solo l'ultimo può essere utilizzato per l'assegnazione degli indirizzi dei PC. Le prime tre parti dell'indirizzo IP di tutti i componenti di rete sono, quindi, sempre uguali.

Switch

Uno switch è simile a un Hub, un elemento per la connessione di diversi segmenti di rete o di componenti di rete. Al contrario di un hub, il commutatore dispone di una propria intelligenza con la quale è in grado di inoltrare i pacchetti solo alla sottorete o al computer allacciato alla rete al quale il pacchetto è destinato.

Vedi anche Bridge, Hub, Router, Gateway

Tariffa flat

La tariffa flat è un tipo di fatturazione per un collegamento Internet. L'Operatore di rete applica una tariffa forfettaria mensile indipendente dalla durata e dal numero di connessioni.

TCP

Transmission Control Protocol

Il protocollo Protocollo TCP appartiene alla famiglia di protocolli TCP/IP. Il TCP esegue il trasporto di dati tra due partner di comunicazione (applicazioni). Per quanto riguarda il TCP, si tratta di un protocollo di trasmissione protetto, questo significa che per la trasmissione dei dati viene aperta, sorvegliata e nuovamente interrotta una connessione.

Vedi anche UDP

TCP/IP

La famiglia di Protocollo su cui si basa Internet. IP costituisce il fondamento di ciascun collegamento tra computer. TCP fornisce alle applicazioni una connessione affidabile di trasmissione sotto forma di flusso di dati continuo. TCP/IP è la base su cui basano servizi quali WWW, mail e news. Esistono anche altri protocolli.

TKIP

Il Temporal Key Integrity Protocol (TKIP) è parte dello standard IEEE 802.11i e viene utilizzato per la crittografia dei dati nelle reti wireless.

UDP

User Datagram Protocol

UDP è un Protocollo della famiglia di protocolli TCP/IP che esegue il trasporto di dati tra due partner di comunicazione (applicazioni). Contrariamente al TCP si tratta di un protocollo non protetto. UDP non stabilisce una connessione fissa. Il pacchetto di dati, il cosiddetto datagramma, viene inviato come Broadcast. Il destinatario è l'unico responsabile della ricezione dei dati. Il mittente non riceve alcun avviso di ricezione.

UPnP

Universal Plug and Play

La tecnologia UpnP è stata concepita per la connessione in rete spontanea di reti domestiche o d'ufficio. Gli apparecchi che supportano UpnP eseguono automaticamente la propria configurazione di rete quando sono collegati a una rete. Essi mettono anche automaticamente a disposizione i propri servizi oppure utilizzano i servizi di altri apparecchi nella rete.

URL

Universal Resource Locator

Indirizzo globale univoco di un dominio in Internet.

WAN

Wide Area Network

Una WAN è una rete a estensione geografica, che non è limitata a un territorio ristretto spazialmente. Internet è la WAN più spesso utilizzata. Una WAN viene gestita da uno o più operatori di rete pubblici che permettono l'accesso a utenti privati. L'accesso a Internet è possibile tramite un Operatore di rete.

WEP

Wired Equivalent Privacy

WEP è un protocollo di protezione che viene definito nello standard IEEE 802.11. Serve a proteggere il traffico in una WLAN contro l'accesso non autorizzato tramite la Crittografia dei dati trasferiti.

WLAN

Wireless LAN

Le LAN wireless (dette reti radio oppure reti wireless) consentono ai componenti della rete la comunicazione con una rete via radio come mezzo di trasporto. Per ampliarla, la wireless LAN può essere collegata a una LAN cablata già esistente oppure può costituire la base per una nuova rete. La particella elementare di una rete wireless è la cosiddetta cella radio. Si tratta dell'area in cui avviene la comunicazione wireless. Una WLAN può essere gestita in Modalità ad hoc oppure in Modalità infrastruttura.

La WLAN è ora definita dallo standard IEEE 802.11. L'hardware del Gigaset SE366 WLAN è conforme allo standard 802.11n (Draft). Un aggiornamento del software viene messo a disposizione dopo il rilascio dello standard.

WPA

Per migliorare la protezione fornita dal WEP è stato sviluppato il WPA. Il WPA utilizza procedure più complesse per la creazione della chiave, quali per es. TKIP (Temporal Key Integrity Protocol). Inoltre, per aumentare la protezione, il WPA può utilizzare un server di autenticazione (ad es. un server RADIUS).

WPA-PSK

WPA Pre-shared Key

Variante della crittografia WPA di dati in cui viene creata automaticamente un nuova chiave con una password (Pre-shared Key) a intervalli regolari. Quindi, la chiave viene rinnovata a intervalli di tempo definiti (Intervallo di rekey).

WPS

Wi-Fi Protected Setup

WPS facilita la realizzazione di reti radio sicure.

WPS imposta le reti radio sicure automaticamente. Gli Punto di accesso generano autonomamente un nome di rete (SSID) e la Crittografia secondo WPA-PSK. I client possono essere così collegati a scelta o tramite la digitazione di un PIN o premendo uno speciale tasto di registrazione nell'Access Point e nel Client.

Indice dei lemmi

A

Accesso a Internet 7
impedire 45
Adattatore di rete 107
wireless 10, 25
Adattatore WLAN. 10
Aggiornamento del firmware. 84
Aggiornare il firmware. 84
Alimentatore
collegare 23
Porta 21
Anti DoS-Firewall. 51
Attacco da parte di un hacker . . 16, 107
avviso via e-mail. 52
Attacco DoS. 51, 107
Avvertenze di sicurezza 6

B

Backup 82
Beacon 107
Bridge 107
Broadcast 67, 107
Browser. 26
BSSID. 108

C

Canale. 66
Cella radio 119
Chiave a 128-Bit 40, 72, 73
Chiave a 64-Bit 40, 72, 73
Chiave ASCII 41, 73
Chiave esadecimale 41, 73
Client 108
Collegamento automatico 108
Collegare il modem via cavo al router 22
Configurazione
ripristino 82
ripristino alle impostazioni iniziali. . 83
Sicurezza 35
Configurazione del blocco dei popup
Windows XP 94
CONFORMITÀ CE 102
Connessione
se necessario 33, 47
Connessione a Internet
disconnettere automaticamente 33, 47
impostare 45
modificare la configurazione. 45
stabilire manualmente 77
terminare manualmente 77
Connessione LAN
creare una connessione via cavo . . . 24
stabilire 24
stabilire wireless 25
connessione manuale 47
Connessione se necessario 108
Contenuto della confezione 18
Controllo di accesso 42, 53, 74
bloccare i servizi 56
Rete locale 74
Controllo di accesso MAC 42, 74
Crittografia. 38, 69, 72, 73, 108
WEP 40
WPA 39
Crittografia a 128 bit 73
Crittografia dei dati 71
Customer Care 104, 105

D

DHCP 108
Digital Subscriber Line vedere DSL
Disattivare il proxy HTTP
Windows XP 93
Disconnettere. 29
Display Login 26
DMZ. 16, 60, 109
DNS 109
Domain Name Service vedere DNS
DSL 109
DTIM 109
Duplex completo 109
Durata della connessione 33
Dynamic DNS vedere DynDNS
Dynamic Host Configuration Protocol
vedere DHCP

DynDNS 61, 110
DynDNS.org 61

E
ECO 6
Elementi di controllo 29
Esadecimale 41, 73
Ethernet 9, 10, 15, 110
  cavo 24
  collegare con una rete wireless 12
  velocità di trasmissione 15
Ethernet 10 Mbit/s 24
Ethernet 100 Mbit/s 24
Exposed Host 16, 60

F
Fast Ethernet 24
file di configurazione 82
Filtro indirizzi MAC 42
Filtro URL 56
Firewall 16, 110
  attivare/disattivare 50
  avviso via e-mail 52
  configurare 50
  definito dall'utente 52
  livello di protezione 52
  protezione dagli hacker 51
Funzioni di sicurezza 13

G
Gateway 110
Gestione remota 80, 110
Gigaset SE336 WLAN
  collegare 22
  collocazione del 21
  configurare 26
  Installazione 17
  lato anteriore 19
  parte posteriore 20
  possibilità di creazione della rete . . . 8
  proteggere con una password 35
Gigaset SE365
  Temperatura ambiente di esercizio . 21
Gigaset SE366 WLAN
  Indirizzo IP 26
Giochi in Internet 57
Guida 29

H
Home 27
Hub 110

I
IEEE 110
Impostazione base 28
  Configurazione 31
  riepilogo 34
Impostazioni internazionali 78
Impostazioni sicurezza 28, 35
  salvare 43
Impostazioni wireless 65
Indirizzo IP 63, 111
  area indirizzi 64
  assegnare in modo statico 64
  dinamico 111
  Gigaset SE336 WLAN 26
  privato 112
  pubblico 112
  statico 112
  utilizzare in automatico 63
Indirizzo IP dinamico 111
Indirizzo IP globale vedere indirizzo IP pubblico
Indirizzo IP locale vedere Indirizzo IP privato
Indirizzo IP privato 112
Indirizzo IP pubblico 112
Indirizzo IP statico 112
Indirizzo MAC 112
  clonare 49
  modificare registrazione 49
Informazioni sullo stato 87
Installazione 17
Institute of Electrical and Electronic Engineers vedere IEEE
Interfaccia DSL
  configurare 31
Interfaccia operativa
  avviare 26
  Pulsanti 29
Interfaccia WAN 11

Internet 112
connessione manuale 47
Connessione se necessario 47
impostare il controllo di accesso . . . 53
Menù 45
modalità di connessione 33, 47
provider di servizi 46
verificare impostazioni 47
Internet Explorer 18, 26
Internet Protocol vedere Protocollo IP
Intervallo di beacon 107
stabilire 67
Intervallo di DTIM 109
stabilire 67
Intervallo indirizzi IP per DHCP 64
Intervallo indirizzi per indirizzi IP 64
IP TV Streaming 15
ISP vedere Operatore di rete

L
LAN 12, 113
lato anteriore 19
LED
comportamento dopo il primo collegamento 25
Registrazione WPS 20, 23
spie 19
Lunghezza della chiave 40
128 Bit (ASCII) 41, 73
128 Bit (esadecimale) 41, 73
64 Bit (ASCII) 41, 73
64 Bit (esadecimale) 41, 73

M
MAC Encapsulated Routing vedere MER
Marchi di fabbrica 6
Maximum Receive Unit vedere MRU
Maximum Transmission Unit vedere MTU
Mbps 113
MER 113
Misure di sicurezza 16
Modalità ad hoc 10, 113
modalità di connessione 33, 47
Modalità di trasmissione 66
duplex 24
semiduplex 24
Modalità infrastruttura 10, 113
Modem DSL
collegare al router 22
Mozilla Firefox 18, 26
MRU 113
MTU 113

N
NAT 56, 114
Port-Forwarding 57
Port-Triggering 57
Network Address Translation vedere NAT
Nome di dominio 114
Numero di porta 60, 114
Corrispondenza 59

O
Open Source Software 106
Operatore 112
Operatore di rete 46, 114
Ora del sistema 79
Ora Internet 79
Ottimizzare le prestazioni della rete . . 67

P
Pagina di registrazione 26
parte posteriore 20
Passphrase 41
Password 26, 35, 36
assegnare 35
cambiare 35
dimenticata 36
modificare 35
Password del sistema
assegnare 79
modificare 79
PBC 13
PIN 14
Point-to-Point Protocol over ATM vedere PPPoA
Point-to-Point Protocol over Ethernet vedere PPPoE
Pool di indirizzi IP 107

Porta 114
LAN 21
per alimentatore 21
per Modem DSL o via cavo 21
porta pubblica 57, 58
Trigger-Port 57, 58
Porta LAN 21
velocità di trasmissione 24
Porta switch 10/100 Mbit/s 21
Port-Forwarding 57, 114
impostare 59
Port-Triggering 57
impostare 58
Potenza di trasmissione 67
PPPoA 114
PPPoE 15, 114
PPPoE Pass-Through 33, 47
Pre-shared Key
Programma di configurazione
avviare 26
Elementi 29
Scelta della lingua 29
Timeout di attesa 80
protezione dagli hacker 51
Protocollo 115
Protocollo IP 113
Proxy HTTP 115
Punto di accesso 10, 65, 115

Q

QoS (Quality of Service) 62

R

Registrazione WPS
Con il PIN dell'apparecchio partner WLAN 69
con PIN dell'Access Point 68
con tasto di registrazione 68
Registrazione, tasto 20
Regola di accesso
Filtro URL 54
Rekeying 39, 69
Repeater 75
Requisiti del sistema 18
Reset 21, 83
Rete 115
Infrastruttura 10
Modalità ad hoc 10
via cavo 9
wireless 10
Rete cablata 9
Rete elettrica, collegamento alla 23
Rete locale 7, 15, 113
Rete radio 119
Modalità ad hoc 10
Modalità infrastruttura 10
Rete wireless
Controllo di accesso 42
Crittografia 38
Nome 13
Riavvio 21, 83
Ricerca degli errori 95
Risoluzione dei problemi 95
Roaming 115
Router 115
impostare la rete locale 8
Indirizzo IP 63
Indirizzo IP dinamico 61

S

Salvare i dati di configurazione 82
Scadenza 64, 115
Semiduplex 116
Server 116
virtuale 116
Server DHCP 64, 108
Server di autenticazione 70
Server di riferimento ora 79
Server DNS 116
definire 49
Server RADIUS 70
Server virtuale 57, 116
Service Set Identifier vedere SSID
Servizi 15
Servizio Clienti 104, 105
Servizio DynDNS vedere DynDNS
Setup avanzato 28
Servizi 44
Simple Mail Transfer Protocol vedere SMTP
Simple Network Management Protocol vedere SNMP
SMTP 116
SNMP 116

Sottorete 117
SPI 117
SSID 17, 37, 66, 117
  invisibile 67
  modificare 37
  preimpostazione sul router 17
  visibile 38, 67
SSID-Broadcast 38, 67
Stateful Packet Inspection 117
Stato
  Apparecchio 92
  panoramica 87
  Rete locale 90
  Rete wireless 91
  Sicurezza 88
Stazione base vedere Punto di accesso
Subnet mask 117
Super G 18
Switch 117
System Log 85

T

Tabella MAC 42
Tariffa flat 117
Tasto di registrazione
  disattivare 86
TCP 117
TCP/IP 118
Temperatura ambiente di esercizio . . 21
Timeout di attesa 80
Tipo di chiave 41
TKIP 119
Transmission Control Protocol vedere TCP
Trigger-Port 57

U

UDP 118
Unione canale 67
Universal Plug and Play vedere UPnP
Universal Resource Locator vedere URL
UPnP 33, 48, 118
  attivare 48
URL 118
User Datagram Protocol vedere UDP

V

VCI 108
velocità di trasmissione 113
  nella LAN Ethernet 15
  nella LAN wireless 15
  Porta LAN 24
Visualizzazione dello stato operativo . 19

W

WAN 118
WDS 75
WEP 38, 40, 69, 71, 118
  Esadecimale 41
  Lunghezza della chiave 40, 73
  modalità di crittografia 72
  Passphrase 41
Wide Area Network vedere WAN
Wi-Fi Protected Setup vedi WPS
Wired Equivalent Privacy vedere WEP
Wireless LAN vedere WLAN
WLAN 10, 12, 119
  modalità operative 10
  velocità di trasmissione 15
WPA 39, 119
  pre-shared Key
WPA2-PSK 38, 70
WPA-PSK 39, 70
WPA-PSK vedere WPA, Pre-shared Key
WPS 13, 35, 68
  Registrazione 68
  Registrazione con PIN 14
  Registrazione tramite tasto 13
  Spia LED durante la registrazione20, 23
  Tasto di registrazione 20

Issued by
Gigaset Communications GmbH
Schlavenhorst 66, D-46395 Bocholt

Gigaset Communications GmbH is a trademark licensee of Siemens AG

© Gigaset Communications GmbH 2008
All rights reserved. Subject to availability.
Rights of modification reserved.

www.gigaset.com

A31008-M1063-R101-4x-7219